

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

SEMESTRÁLNÍ PRÁCE



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

**FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ**

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

**APLIKACE PRO GENEROVÁNÍ A OVĚŘOVÁNÍ
KONFIGURACÍ SÍŤOVÝCH ZAŘÍZENÍ**

APPLICATION GENERATING AND VERIFYING CONFIGURATIONS OF NETWORK DEVICES

SEMESTRÁLNÍ PRÁCE

SEMESTRAL THESIS

AUTOR PRÁCE

AUTHOR

Bc. Juraj Korček

VEDOUCÍ PRÁCE

SUPERVISOR

doc. Ing. Jan Jeřábek, Ph.D.

BRNO 2019

Semestrální práce

magisterský navazující studijní obor **Informační bezpečnost**

Ústav telekomunikací

Student: Bc. Juraj Korček

ID: 187238

Ročník: 2

Akademický rok: 2019/20

NÁZEV TÉMATU:

Aplikace pro generování a ověřování konfigurací síťových zařízení

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s problematikou síťových zařízení, síťových operačních systémů, hlavních používaných komunikačních protokolů a způsobů konfigurace těchto zařízení. Dále prostudujte problematiku osvědčených postupů konfigurace, zejména s ohledem na bezpečnost fungování zařízení v síti a také problematiku anonymizace těchto konfigurací. Navrhněte systém či aplikaci, která bude umět pro vybranou množinu síťových zařízení vytvářet přednastavené parametry nastavení, které bude možné na dané síťové zařízení aplikovat. Dále musí daná aplikace umět verifikovat správnost existujících konfigurací, upozornit na případné nedostatky a i konfiguraci modifikovat tak, aby splňovala hlavní bezpečnostní a provozní standardy a doporučení. Fungování aplikace ověřte na testovacích vzorcích síťových konfigurací různých zařízení z několika různých sítí a případně i různých výrobců.

V rámci semestrálního projektu je třeba vypracovat teoretickou část zadání, vybrat vhodné programovací prostředí pro plánovanou aplikaci a navrhnout a popsat strukturu dané aplikace či systému, včetně základního popisu jednotlivých komponent a jejich předpokládané funkcionality. Vlastní řešení mírně rozpracujte.

DOPORUČENÁ LITERATURA:

[1] Stallings W., Network security essentials: applications and standards. 6th ed. Hoboken: Pearson education, 2017, 445 s. ISBN 978-0-13-452733-8.

[2] McMillan, T., CCNA Security Study Guide: Exam 210-260. 2nd ed. USA: Sybex, 2018, 384 s. ISBN 978-1--1-940993-9.

Termín zadání: 23.9.2019

Termín odevzdání: 21.12.2019

Vedoucí práce: doc. Ing. Jan Jeřábek, Ph.D.

Konzultant:

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

UPOZORNĚNÍ:

Autor semestrální práce nesmí při vytváření semestrální práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

VYHLÁSENIE

Vyhlasujem, že svoju semestrálnú prácu na tému „Applikace pro generování a ověřování konfigurací síťových zařízení“ som vypracoval samostatne pod vedením vedúceho semestrálnej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej semestrálnej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto semestrálnej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno

.....

podpis autora

Obsah

Úvod	9
1 Kybernetická bezpečnosť	10
1.1 Vybrané pojmy z kybernetickej bezpečnosti	10
1.2 Ciele sieťovej bezpečnosti	11
1.2.1 Triáda CIA	12
1.3 Pasívne a aktívne útoky	13
2 Bezpečnostný audit	16
2.1 Manažment rizík	17
3 Prevádzka a bezpečnosť sietí	19
3.1 Sieťové prvky	19
3.2 Hierarchický model sietí	19
3.3 Funkčné roviny sieťových prvkov	21
3.4 Prevádzkové a bezpečnostné postupy	22
4 Návrh	42
4.1 Požiadavky na aplikáciu a existujúce riešenia	42
4.2 Rozdelenie príkazov	44
4.3 Rozdelenie sieťových prvkov	45
4.4 Princíp fungovania	45
4.5 Zoznam odporúčaní	49
5 Implementácia	71
5.1 Použité technológie	71
5.1.1 Python	71
5.1.2 YAML	71
5.1.3 Regulárne výrazy	71
5.2 Konfiguračné súbory	71
5.2.1 Súbor popisujúci zariadenie	71
5.2.2 Súbor popisujúci modul	71
5.3 Moduly	71
Záver	72
Literatúra	73
Zoznam symbolov, veličín a skratiek	77

Zoznam príloh	79
A Zdrojové súbory	80
A.1 Konfiguračné súbory	80
B Checklist	81

Zoznam obrázkov

1.1	Koncept bezpečnosti a vzájomné vzťahy pojmov	11
1.2	Triáda dôvernôst, integrita a dostupnosť	12
1.3	Pasívny útok	13
1.4	Aktívny útok maškaráda	14
1.5	Aktívny útok DOS	14
1.6	Aktívny útok modifikácia správy	14
1.7	Aktívny útok prehratím	15
3.1	Typy sieťových zariadení v lokálnych sieťach	19
3.2	Hierarchické rozdelenie siete na vrstvy	20
3.3	Rozdelenie rovín v smerovači, tok informácií v jeho vnútri a medzi susednými smerovačmi	22
3.4	Prihlasovanie k manažmentu zariadenia z povolených IP adries a lo- govanie pokusov z nepovolených IP adries	23
3.5	Overenie prihlásenia k manažmentu zariadenia pomocou AAA serveru	24
3.6	Blokovanie správ dynamického smerovacieho protokolu na pasívne ro- zhranie	26
3.7	Porovnanie prístupov TTL security	27
3.8	Ilustrácia aplifikačného útoku cez nakazený počítač pomocou podvr- hnutej IP adresy	30
3.9	Zabránenie prebratia role Root Bridge pomocou Root Guard	32
3.10	Zabránenie vyhlásenie koncového portu ako portu k prepínaču pomo- cou BPDU Guard	32
3.11	VLAN Hopping s Double Tagging	33
3.12	Útok Switch spoofing pomocou protokolu DTP	33
3.13	Autentizácia 802.1x zjednodušené	35
3.14	DHCP Snooping a IP Source Guard	37
3.15	Porovnanie site-to-site a remote access VPN	40
4.1	Vývojový diagram opisujúci prácu s programom a tok dát v programe	46

Zoznam tabuliek

4.1	Odporúčania k prístupu na manažment zariadení	55
4.2	Odporúčania pre smerovanie	56
4.3	Odporúčania pre filtrovanie prevádzky	57
4.4	Odporúčania pri vysokom zaťažení	58
4.5	Odporúčania na zamedzenie mapovanie siete	59
4.6	Odporúčania na identifikáciu zariadení a nastavení	60
4.7	Odporúčania k protokolu NTP	61
4.8	Odporúčanie pre protokol SNMP	62
4.9	Odporúčania pre protokol Syslog	63
4.10	First Hop Security útoky a odporúčania	66
4.11	Odporúčania pre Spanning Tree Protokol	67
4.12	Odporúčania pre VLAN	68
4.13	Ostatné nezatriedené odporúčania	70

Zoznam výpisov

4.1	Konfigurácia verzie protokolu SSH	44
4.2	Konfigurácia maximálneho počtu povolených MAC adries na porte . .	44
4.3	Konfigurácia autentizácie OSPF na porte alebo v proccese	44
4.4	Konfigurácia protokolu LLDP a vypnutie protokolu pre jeden port . .	45

Úvod

Kybernetická bezpečnosť je bezpochyby jednou z hlavných tém 21. storočia. Útoky na infraštruktúru a systémy naberajú nielen na frekvencii, ale čo je ešte horšie na sofistikovanosti. Napriek častému zdôrazňovaniu odborníkov o kladenie čoraz väčšieho dôrazu na bezpečnosť pri návrhu, implementácii a nasadení, sa stále stretávame s fatálnymi dôsledkami, ktoré boli spôsobené nedostatočným venovaním pozornosti bezpečnosti.

Problém nedostatočného zabezpečenia nie je ani tak nevedomosť základných bezpečnostných praktík administrátorov alebo programátorov, ale potreba rýchleho nasadenia systému a infraštruktúry s odložením implementácie bezpečnostných praktík na neskôr. Tieto problémy vznikajú aj pri dodatočnej implementácii nových modulov a pridaní novej infraštruktúry, kedy sa nemení celok, ale pridanie jednej časti môže výrazne ovplyvniť a zmeniť stav bezpečnosti celého systému. Z tohto dôvodu je priam žiadúce disponovať nejakým procesom alebo nástrojom na dodatočné zistenie nedostatkov a ich následnú elimináciu. Veľmi silnou motiváciou by malo byť aj to, že dôsledkom bezpečnostných nedostatkov sú globálne miliardové škody a straty reputácií firiem.

Jednou z hlavných častí infraštruktúry, kde dochádza k významným bezpečnostným incidentom je počítačová sieť, bez ktorej by dnes informačné technológie nevedeli fungovať. Preto sa táto práca bude zaoberať práve ňou, keďže je vstupnou bránou do systémov a jej vyradením alebo zneužitím prichádzajú organizácie o finančné prostriedky, citlivé dáta a dôveru užívateľov.

Výsledkom tejto práce bude aplikácia overujúca nastavenia sieťových zariadení prevažne v lokálnej sieti, ktorá umožňuje zjednať nápravu na základe nájdených nedostatkov. Výhodou oproti existujúcim riešeniam bude otvorenosť kódu a modularita, ktorá umožní rozšírenie aplikácie na sieťové zariadenia rôznych výrobcov. Dôležitým výstupom bude taktiež zoznam bezpečnostných a prevádzkových odporúčaní vychádzajúcich z rôznych štandardov a odporúčaní, ktoré môžu byť v budúcnosti použité ďalšími užívateľmi aplikácie pri zostavovaní modulov pre zariadenia rôznych výrobcov. Jednou z kľúčových vlastností je bezplatnosť, keďže podľa zistení takmer polovica útokov smeruje na malé firmy, ktoré bezpečnosť často neriešia z finančnej náročnosti programov na detekciu bezpečnostných nedostatkov.

1 Kybernetická bezpečnosť

S čoraz na väčšou informatizáciou naprieč všetkými odvetviami života, je nutnosťou riešiť aj zabezpečenie systémov, infraštruktúry a dát. Kybernetická bezpečnosť je bez pochyb jednou z najdiskutovanejších tém 21. storočia.

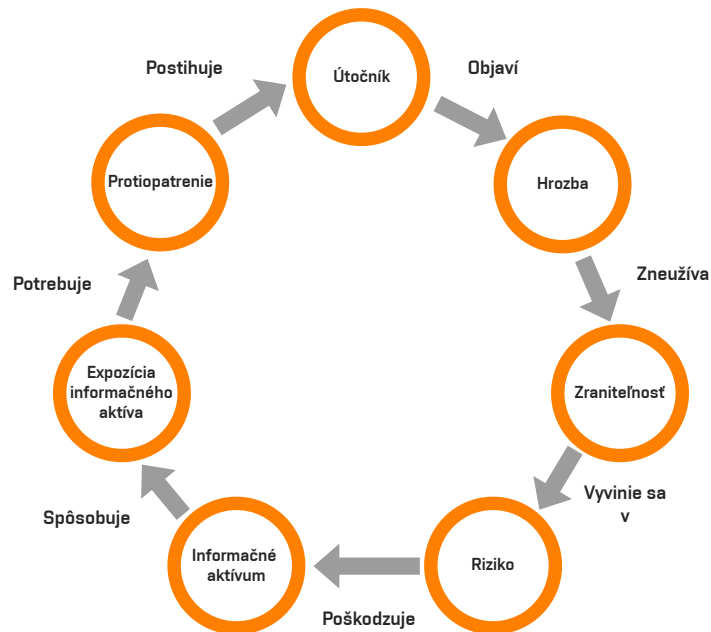
Podľa zistení z roku 2018 [1] takmer polovica útokov smeruje na malé firmy, ktoré bezpečnosť riešia iba minimálne alebo vôbec. Predpokladá sa [1], že pre rok 2019 bude na kybernetickú bezpečnosť minútých 6 miliárd dolárov, naopak škody spôsobené kybernetickými útokmi presiahnu jednu miliardu dolárov a veľmi záškodné útoky typu *Distributed Denial of Service* – *distribúované odoprenie služby* (DDoS) by mali vzrásť až šesťnásobne.

Vyššie zmienené predpovede len potvrdzujú dôležitosť kybernetickej bezpečnosti pri návrhu, implementácii, nasadzovaní a prevádzke informačných technológií.

1.1 Vybrané pojmy z kybernetickej bezpečnosti

- Informačné aktívum (Asset) – čokoľvek, čo je nutné chrániť, napr. dáta, fyzická informačná infraštruktúra, systémy [3].
- Zraniteľnosť (Vulnerability) – neprítomnosť alebo nedostatočné opatrenia na zabezpečenie. Zraniteľnosť môže byť prítomná hardvéri, softvéri alebo samotnom užívateľovi [3].
- Hrozba (Threat) – vzniká v prípade odhalenia alebo zneužitia zraniteľnosti. Zároveň platí, že hrozbou je aj zraniteľnosť, ktorá doposiaľ nebola neidentifikovaná [3].
- Útočník (Threat agent) – entita, ktorá zneužije zraniteľnosť [3].
- Riziko (Risk) – pravdepodobnosť, že útočník využije zraniteľnosť, pričom príde k dopadu na systém alebo infraštruktúru [3].
- Útok na bezpečnosť (Security attack/Exploitation) – krok, ktorý kompromituje bezpečnosť informačného aktíva [2].
- Bezpečnostný mechanizmus (Security mechanism) – proces, ktorý je navrhnutý na detegovanie, prevenciu a zotavenie z útoku na bezpečnosť.

- Protiopatrenie (Countermeasure) – ochranné opatrenie, ktoré znižuje riziko [3].
- Expozícia informačného aktíva (Exposure) – dochádza k nej ak je aktívum vystavené stratám nedostatočným alebo neprítomným zabezpečením [3].



Obr. 1.1: Koncept bezpečnosti a vzájomné vzťahy pojmov [3]

Na obrázku 1.1 je možné vidieť vzájomnú interakciu medzi pojmi. Zároveň je nutné si uvedomiť, že takýto cyklus nie je v systéme alebo infraštruktúre jeden a taktiež môže vzniknúť niekoľko paralelných cyklov pričom každý môže mať počiatok v inom uzle. Je dobré myslieť na to, že jednotlivé cykly môžu na seba vplývať, napríklad jedno protiopatrenie môže postihnúť viacero útočníkov využívajúcich rôzne hrozby.

1.2 Ciele sieťovej bezpečnosti

Bezpečnosť počítačovej siete, tak ako aj iných podoblastí kybernetickej bezpečnosti je založená na troch základných princípoch známych ako *confidentiality*, *integrity*, *availability* – *dôvernosť*, *integrita*, *dostupnosť* (CIA). Bezpečnosť musí pokryť všetky tri aspekty popísané týmto modelom, pričom narušenie čo i len jednej zložky má za následok nesplnenie celkového zabezpečenia [2].

1.2.1 Triáda CIA

Triáda CIA pozostáva z nasledujúcich častí [3]:

- Confidentiality (Dôvernosť) – zabránenie prístupu k dátam alebo informáciám neoprávneným osobám. Na zaistenie tejto požiadavky sa najčastejšie používa šifrovanie, ale aj autentizácia a autorizácia. Jej strata vedie k neoprávnenému zverejneniu informácií.
- Integrity (Integrita) – dáta alebo informácie sú zabezpečené proti neautorizovanej modifikácii a poškodeniu. Týmto zaistujem konzistenciu dát pri prenose alebo uchovaní na médiu. Integritu zaistujeme hašovacími funkciami prípadne za pomoci *Access Control List* – zoznam pre riadenie prístupu (ACL).
- Availability (Dostupnosť) – dáta alebo informácie sú dostupné iba pre určité entity v daný čas a miesto.



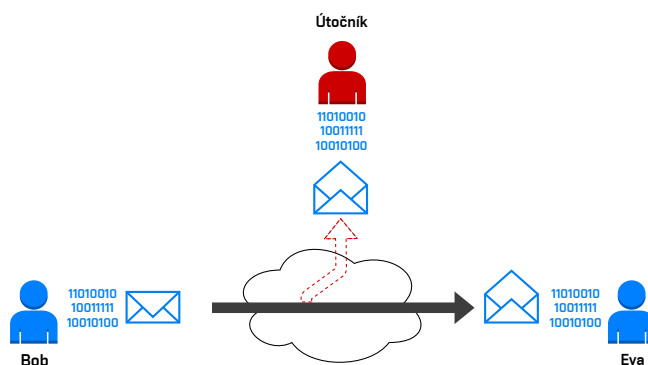
Obr. 1.2: Triáda dôvernosť, integrita a dostupnosť demonštrujúca potrebu všetkých troch prvkov na zaistenie bezpečnosti [2]

Aj keď triáda CIA definuje ciele na zaistenie bezpečnosti, tak niektorí odborníci ju nepovažujú za dostatočnú a zavádzajú ďalšie dve podmienky a pojmy [4]:

- Authencity (Autenticita) – overenie originality a platnosti správy a identity jej pôvodcovi. Najčastejšie sa na zaistenie tejto podmienky využívajú certifikáty.
- Accountability (Sledovateľnosť) – identifikácia prístupu k informáciám a vysledovateľnosť bezpečnostných incidentov v prípade využitia forenzej analýzy. Väčšinou je táto požiadavka zaistená záznamom činnosti v systéme formou logu.

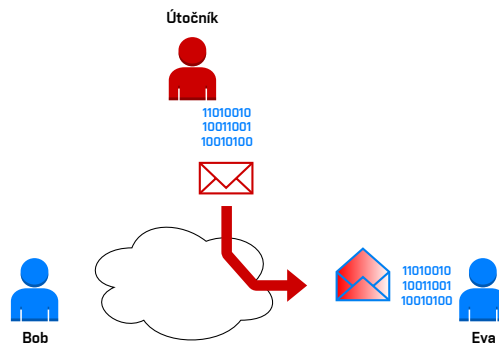
1.3 Pasívne a aktívne útoky

Útoky na bezpečnosť môžu byť rozdelené do dvoch skupín [2]. Jednou skupinou je pasívny útok, kde nepozmeňuje útočník pôvodné dáta a nevplýva na príjemcu týchto dát. Druhou možnosťou je aktívny útok, pri ktorom sú buď pozmenené dáta doručené príjemcovi alebo je obeť nejakým spôsobom ovplyvňovaná, napríklad zasielaním falošných informácií.

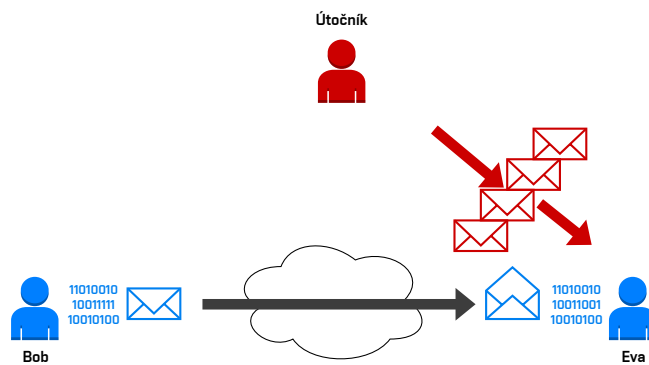


Obr. 1.3: Príklad pasívneho útoku, pri ktorom útočník odpočúva komunikáciu medzi dvoma uzlami [4]

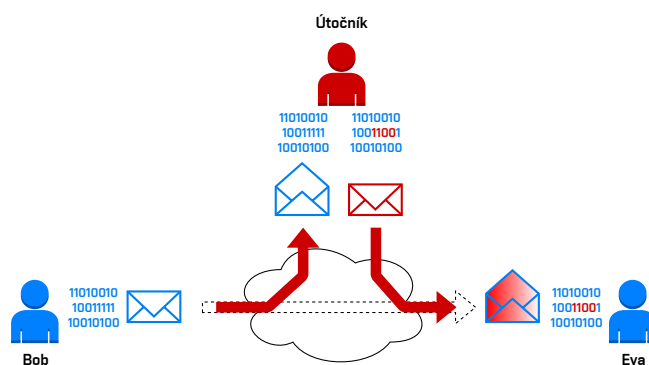
Pri pasívnom útoku, ktorý je znázornený na obrázku 1.3 ide útočníkovi prevažne o zachytenie prenášanej komunikácie a monitorovanie a analýzu prevádzky. Odposluch a zobrazenie obsahu dát je účinné hlavne pri nepoužití šifrovania správ medzi koncovými bodmi alebo aj pri použití slabých šifier, krátkych kľúčov a nedostatočne bezpečných hesiel. Monitorovanie prevádzky, respektíve analýza komunikácie je možná aj pri použití šifrovania, keďže každá komunikácia je charakteristická určitým vzorom. Pasívne útoky je nesmierne obtiažne detegovať nakoľko nemodifikujú dáta pri prenose. Najúčinnnejšia obrana je použitie dostatočne silných šifier na zabezpečenie dát. Jeden z pasívnych útokov sa hojne využíva aj pri prevencii v *Intrusion Detection System* – *systém detekcie narušenia* (IDS) a *Intrusion Prevention System* – *systém prevencie prienikov* (IPS), kde bez analýzy prevádzky by nebolo možné zabezpečiť sieť. Pasívnymi útokmi sa nespôsobuje škoda na systéme alebo infraštruktúre, ale hrozba spočíva v narušení dôvernosti.



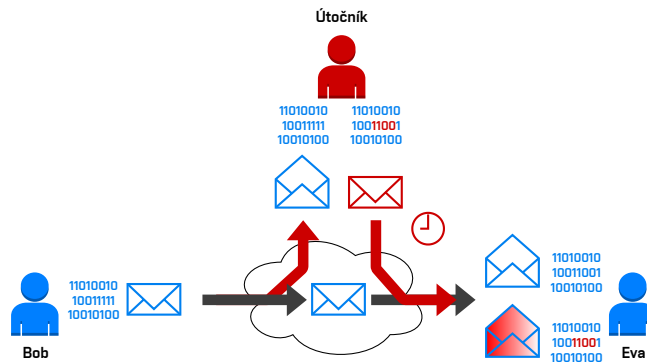
Obr. 1.4: Príklad aktívneho útoku maškarádou, kedy uzol Eva obdrží falošnú správu od útočníka mysliac si, že ide o správu od uzla Bob [4]



Obr. 1.5: Príklad aktívneho útoku DOS, pri ktorom je uzol Eva zahltený nevyžiadanými správami (označené červeno) [4]



Obr. 1.6: Príklad aktívneho útoku modifikáciou správy, pri ktorom je originálna správa presmerovaná cez útočníka, následne pozmenená a prijatá uzlom Eva, ktorý ju považuje za legítimnú [4]



Obr. 1.7: Príklad aktívneho útoku prehratím, pri ktorom príde uzlu Eva legitímna správa (označená modro) a následne po určitom čase aj odchytená správa od útočníka, ktorá je pozmenená (označená červeno) [4]

Aktívne útoky sú sofistikovanejšie ako pasívne, modifikujú dáta alebo vytvárajú falošné, o ktorých prijímateľ predpokladá, že prišli od zdroja, s ktorým pôvodne komunikoval. Hrozby, ktoré môžu týmito útokmi nastať sú strata integrity, teda modifikácia dát a ohrozenie dostupnosti pričom vždy dochádza ku škode na systéme alebo infraštruktúre. Maškaráda je prvým z aktívnych útokov, kde ako je možné vidieť na obrázku 1.4, útočník vytvára falošnú správu, ktorú zasiela obeti a tá sa domnieva, že komunikuje s pôvodným zdrojom, v našom prípade Bobom. Použitím osobných certifikátov na oboch stranách by bolo možné odhaliť, že správa nepochádza od zdroja, ale od útočníka. Príkladom aktívneho útoku je aj útok odoprenia služby 1.5, kde sa vytvárajú falošné dáta generované vysokou frekvenciou, v obrázku značené červenou farbou, za účelom odstaviť systém alebo infraštruktúru, ktorá nezvláda spracovanie toľkých požiadaviek, keďže nebola na takúto záťaž dimenzovaná. Tretím aktívnym útokom 1.6 je modifikácia správy útočníkom pri prechode komunikačným kanálom, ktorý sa realizuje rôznymi technikami podvrhnutia zdroja alebo identity. Komunikácia v tomto prípade prebieha cez útočníka, ktorý tento útok mohol uskutočniť napríklad podvrhnutím smerovania. Posledným útokom je útok prehratím 1.7, čo je útok veľmi podobný predchádzajúcemu, akurát obeť obdrží najprv pôvodnú nepozmenenú správu a následne po určitom čase aj modifikovanú správu od útočníka. Takéto správy môžu byť generované aj ako nežiadúca sieťová prevádzka pri zahľtení prvkov alebo pri zlom nastavení smerovania. Citlivé sú najmä tranzakčné systémy napríklad databáze. Zabrániť tomuto útoku je možné pomocou časových pečiatok a jednoznačných identifikátorov.

2 Bezpečnostný audit

Auditovanie je veľmi dôležitým prvkom správy informačných systémov a infraštruktúry, pretože umožňuje zaistiť bezpečnosť týchto informačných aktív porovnávaním s vytvorenými štandardmi, odporúčaniami a predpismi. Zaoberá sa otázkami čo a ako zabezpečiť, vyhodnocovaním a riadením rizík a následným dokazovaním, že náprava znížila riziko hrozby.

Auditovanie sa skladá z piatich pilierov [5]:

1. Posúdenie
2. Prevencia
3. Detekcia
4. Reakcia
5. Zotavenie

Pri posudzovaní si je potreba klásť otázky či sú prístupové práva dostatočne špecifikované, aká je pravdepodobnosť útoku na zraniteľnosť a podobne. Prevencia nespočíva iba v technológiách ako firewall prípadne IDS a IPS, ale aj v politikách, procesoch a povedomí o probléme. Detekcia a reakcia spolu úzko súvisia a je potrebné skrátiť dobu medzi týmito dvoma bodmi, bez dôkladnej detekcie nie je možné vykonať reakciu. Mnohé reakcie na detekciu problému sú už rôznymi technológiami implementované automatizovane. Posledný článkom je zotavenie, ktoré je dôležité pri službách vysokej dostupnosti. Výborným príkladom detekcie, reakcie a zotavenia z problému sú protokoly z rodiny *First Hop Redundancy Protocol* (FHRP).

Proces auditu pozostáva z niekoľkých fází: [5]

1. Plánovanie – stanovenie cieľov a predmetu auditu. Definuje sa rozsah, teda čo všetko je v pláne auditom pokrytý.
2. Výskum – vytváranie auditného plánu na základe štandardov a odporúčaní a špeciálnych expertíz. Kontaktujú sa tiež dotknuté strany, ktoré nám môžu byť nápomocné pri plnení cieľov.
3. Zbieranie dát – vyžiadanie potrebných podkladov a dát na vykonanie auditu, zozbieranie dôkazov. V tejto fáze sa tiež vyberajú rôzne softvérové nástroje na vykonanie auditu a vytvorí sa checklist na základe auditného plánu a zozbieraných dôkazov.
4. Analýza dát – posúdenie všetkých dôkazových dát pomocou checklistu a softvéru na podporu auditu. Na základe nájdených nedostatkov sa vytvoria odporúčania, ktoré by mali znížiť riziká hrozieb.
5. Vytváranie správy – súpis nájdených nedostatkov, možných riešení na zníženie rizík do auditnej správy a prezentácia tejto správy dotknutým stranám.

6. Aplikácia opatrení – nasadenie a použitie protiopatrení prezentovaných alebo vyplývajúcich z auditnej správy. Následne sa môže vykonať monitorovanie a hlásenie o úspešnosti zmien.

Typy auditov podľa zistení, hĺbky a rozsahu auditu:

- Bezpečnostná kontrola – je najzákladnejšia forma analýzy bezpečnosti, na základe ktorej sa následne formujú ďalšie aktivity na zaistenie bezpečnosti. Do tejto kategórie spadajú automatizované nástroje na skenovanie zraniteľností a penetračné nástroje, ktoré generujú zoznam potenciálnych zraniteľností, ale je potrebné ďalšie podrobnejšie preskúmanie výsledkov a zistení a stanovenie, ako sa k nim zachovať. Patria sem nástroje ako napríklad Nmap, Nessus a podobne. Za bezpečnostnú kontrolu možno považovať preskúmanie politík alebo architektúry daného systému a infraštruktúry. Dá sa povedať, že ide o akýsi rýchly náhľad na bezpečnosť, ktorého výstupom je poznanie a identifikovanie problému.
- Hodnotenie bezpečnosti – je ďalším stupňom, pričom ide o podrobnejší pohľad na problém z profesionálnejšieho hľadiska. Kvalifikuje sa riziko k jednotlivým zisteniam a stanovuje sa relevantnosť a kritickosť týchto zistení na konkrétnu organizáciu a prípad použitia.
- Bezpečnostný audit – je štandardizovanou a najdôkladnejšou formou posúdenia bezpečnosti. Bezpečnosť sa porovnáva so štandardmi alebo benchmark-mi, v niektorých prípadoch aj s predpismi dohliadahúcich orgánov. Výsledkom je posúdenie, na koľko je organizácia alebo skúmaný objekt v zhode s porovnávaným štandardom. Typickým príkladom štandardov sú ISO27001 a COBIT.

2.1 Manažment rizík

Manažment rizík je proces pozostávajúci z analýzy rizík a riadenia rizík [3]. Dôležitým faktom je, že riziko nie je možné eliminovať, ale ho iba znížiť.

Pri analýze rizík zisťujeme, aké riziká existujú, ako medzi sebou súvisia a aké škody môžu spôsobiť. Analýza rizík môže byť vykonávaná kvalitatívne a kvantitatívne.

Štandard NIST SP 800-30 [6] definuje nasledujúce kroky pri analýze rizík:

1. Identifikácia informačných aktív a ich význam
2. Identifikácia hrozieb
3. Identifikácia zraniteľností
4. Analýza riadenia a kontroly
5. Zistenie pravdepodobnosti
6. Identifikovanie dopadu
7. Definovanie rizika ako súčinu pravdepodobnosti a dopadu
8. Odporúčanie na zavedenie riadenia a kontroly na zníženie rizika
9. Zdokumentovanie výsledkov

Riadenie rizík má za úlohu minimalizáciu potenciálnych škôd odhalených pri analýze rizík s ohľadom na vyváženú nákladov na riadenie rizika.

Prístupy k nájdenému riziku [2][3][5]:

- Vyhnutie sa riziku – je uplatnené ak prítomnosť a funkčnosť informačného aktíva nestojí za podstúpenie rizika, a teda toto aktívum vôbec nepoužijeme. Napríklad vypnutie menej bezpečných a nevyužívaných sieťových služieb.
- Zníženie – aplikovanie protiopatrenia na odstránenie hrozby alebo zraniteľnosti prípadne zníženie pravdepodobnosti rizika. Nikdy nie je však možné riziko eliminovať. Príkladom môže byť obmedzenie prístupu k sieťovému prvku.
- Akceptovanie – v prípade neexistujúceho protiopatrenia alebo veľmi nízkeho rizika. Často ide o bezpečnostnú chybu softvéru v službe, ktorú využívame a nie je možné ju vypnúť ani aplikovať protiopatrenie.
- Presun – riziko je možné presunúť na inú organizáciu, napr. poistenie v prípade škody spôsobenej nedostatočným zabezpečením.
- Ignorácia – úplné vypustenie faktu, že dochádza k riziku, tento prístup sa považuje za iracionálny.

Na ohodnotenie rizika slúžia rôzne systémy hodnotenia, jedným z nich je *Common Vulnerability Scoring System* (CVSS), ktorý definuje riziká podľa definovaných metrick na základe dosiahnutého skóre do nasledujúcich tried:

- 0: No issue
- 0,1 – 3,9: Low
- 4,0 – 6,9: Medium
- 7,0 – 8,9: High
- 9,0 – 10,0: Critical

3 Prevádzka a bezpečnosť sietí

Prevádzka sieťových zariadení je proces nielen o monitorovaní incidentov, zabezpečovaní konzistencie a konvergenzie siete, ale aj o aktualizáciách softvéru a hardvéru, aplikovaní bezpečnostných zásad a politík. Táto kapitola preto opisuje jednotlivé aspekty s ktorými sa pri prevádzke siete môžeme stretnúť.

3.1 Sieťové prvky

Medzi základné stavebné piliere sietí, bez ktorých nie je možná komunikácia koncových staníc patria smerovače (router) a prepínače (switch). Mimo týchto dvoch základných zariadení sa v *Local Area Network* (LAN) sieťach často vyskytujú prístupové body (access point), firewally, sieťové mosty (bridge) a v dnes už ojedinelých prípadoch ešte aj rozbočovače (hub). V súčasnosti však jedno zariadenie môže kombinovať funkcie zariadení, ktoré majú podľa modelov TCP/IP alebo ISO/OSI na starosti inú vrstvu modelu. Preto sa dnes hlavne z finančných dôvodov používajú takzvané L3 prepínače, ktoré s určitými obmedzeniami vedia nahradiť nákladné smerovače. Taktiež smerovače ako aj L3 prepínače umožňujú filtrovanie paketov, takže vedú čiastočne zastaať aj základné funkcie firewallu. Značky najpoužívanejších sieťových zariadení su vyobrazené na obrázku 3.1 a budú používané v nasledujúcich kapitolách.



Obr. 3.1: Typy sieťových zariadení v lokálnych sieťach

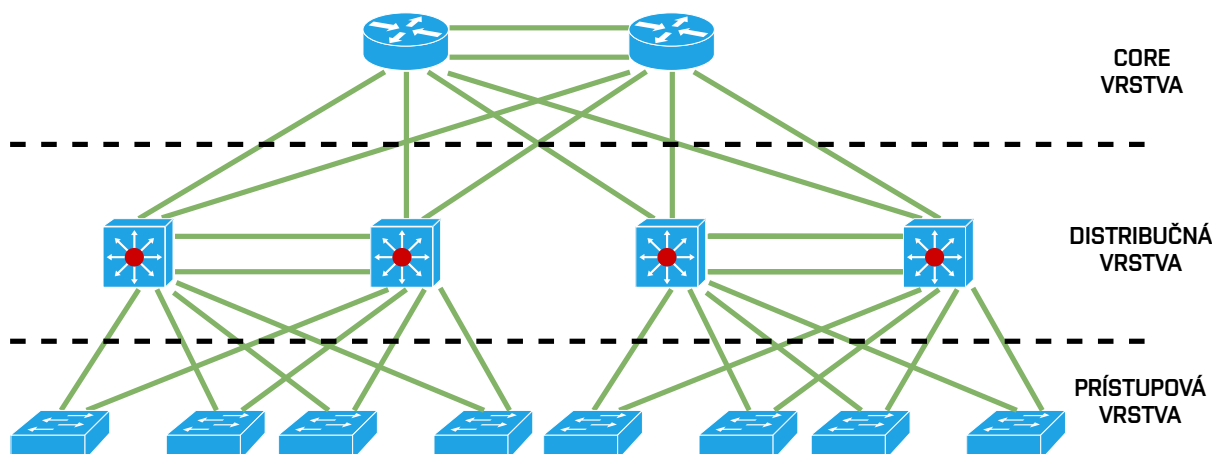
3.2 Hierarchický model sietí

S postupným nárastom sieťových zariadení a komplexnosti siete dochádza v sieťach bez hierarchie k mnohým problémom ako veľké broadcast domény, vysoká cena za

port, vysoké zaťaženia zariadení, neprítomnosť redundancie. Preto sa zaviedol hierarchický model siete, ktorý rieši problémy veľkosti a rozsahu broadcast a kolíznych domén, umožňuje efektívne pridelovanie *Internet Protocol* (IP) adres a oddeľuje zariadenia pracujúce na jednotlivých vrstvách ISO/OSI.

Siete sú spravidla delené do 3 vrstiev s definovanými funkciami [8]:

- Core – tvorí vysokorýchlostnú chrbticu siete, agreguje dáta z distribučnej vrstvy a mala by byť redundantná. Nároky na rýchlosť portov a výkon zariadenia sú obzvlášť vysoké, a preto sa využívajú prevažne smerovače, ale taktiež ako v distribučnej vrstve dnes už aj L3 prepínače.
- Distribučná (Distribution) – agreguje dáta z prístupovej vrstvy, vytvára a oddeľuje broadcast domény, riadi smerovanie medzi *Virtual LAN* (VLAN) a filtrovanie paketov. Táto vrstva kvôli zabezpečeniu dostupnosti využíva agregovanie a redundanciu liniek. Typicky sa skladá zo smerovačov, no v dnešnej dobe hlavne z L3 prepínačov, keďže tie nie sú finančne také náročné.
- Prístupová (Access) – vstupný bod do siete, ktorý riadi prístup a politiku pre koncové zariadenia, segmentuje sieť, vytvára a separuje kolízne domény. V neposlednej rade zariaďujú prístup k distribučnej vrstve. Je tvorená zariadeniami ako prepínač, rozbočovač alebo prístupový bod.



Obr. 3.2: Hierarchické rozdelenie siete na vrstvy

V menších sieťach prevažne malých firiem sa využíva zlučovanie vrstiev nazývaných

ako collapsed core, ktoré zlučujú distribučnú a core vrstvu, prípadne zlučujú všetky tri vrstvy dokopy.

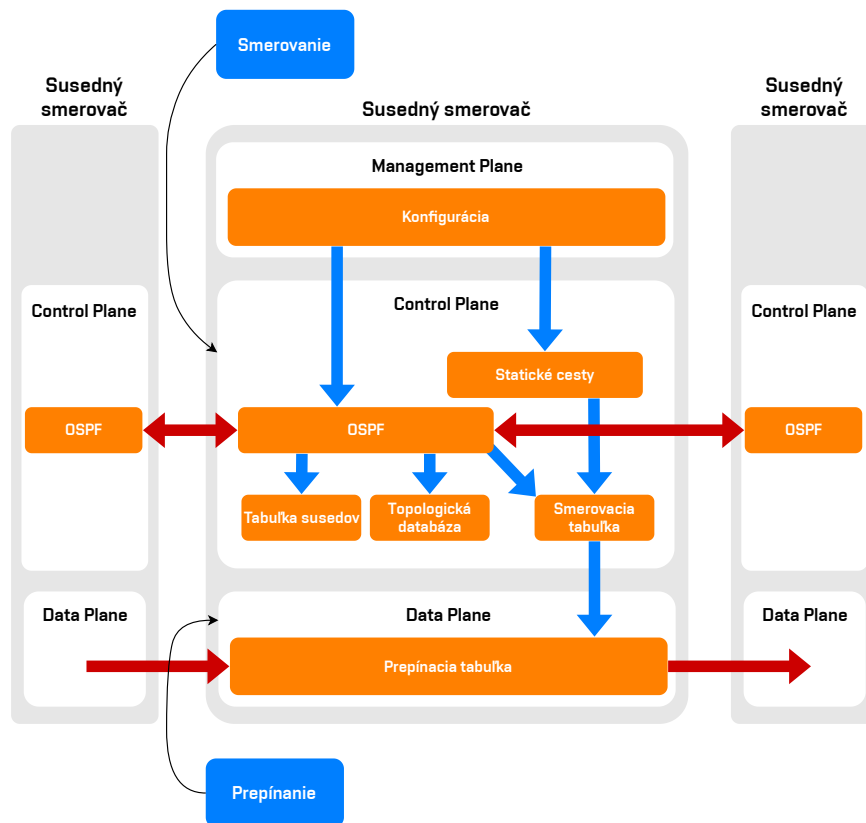
Cieľom hierarchického modelu a dobre navrhnutej siete je dosiahnutie nasledujúcich vlastností:

- Škálovateľnosť – jednoduché a bezproblémové pridanie zariadenia pri raste a rozširovaní siete.
- Redundancia – zabezpečenie vysokej dostupnosti viacnásobnými linkami medzi zariadeniami a zálohovanie samotných zariadení ich redundanciou.
- Výkonnosť – agregovanie liniek a výber dostatočne výkonných zariadení
- Bezpečnosť – zabezpečenie siete na viacerých úrovniach ako napríklad portoch, oddelením segmentov pomocou VLAN, riadením prístupu, šifrovaním a pod.
- Manažovateľnosť – vytvorenie šablón, definovaných štandardov a pravidiel na zaistenie konzistentnosti konfigurácií zariadení na jednoduchšie odhaľovanie chýb.
- Udržovateľnosť – schopnosť systému prechádzať zmenami komponentov, služieb a vlastností.

3.3 Funkčné roviny sieťových prvkov

Sieťové prvky sú zodpovedné nielen za preposielanie dát medzi koncovými stanicami, ale aj za mnohé riadiace dáta medzi sebou, bez ktorých by sieť nebola funkčná. Preto sa jednotlivé protokoly a služby rozdeľujú troch rovín, a to management, control a data plane. Tieto pojmy sa využívajú vo väčšej miere v softvérovo definovaných sieťach, no sú platné aj v klasickej koncepcii.

Rovina management je zodpovedná za konfiguráciu a správu zariadení a riadenie prístupu ku konfiguráciám. Typickými príkladmi protokolov pracujúcich na tejto rovine sú *Simple Network Management Protocol* (SNMP), *Authentication Authorization Accounting* (AAA), Syslog, *Secure Shell* (SSH) a mnohé ďalšie [7]. Druhá rovina, control plane má na starosti prevažne riadenie siete a smerovanie. Zaoberá sa otázkou kadiaľ budú pakety smerované a prenáša riadiace a signalizačné informácie pre protokoly ako napríklad, *Open Shortest Path First* (OSPF), Spanning tree, FHRP [7]. Poslednou rovinou je data plane nazývaná často aj forwarding plane, ktorá prepína pakety na daný port na základe rozhodnutia z control plane. Táto časť sieťových prvkov musí byť veľmi rýchla, aby zaistila nízku odozvu a dostatočne vysoké prenosové rýchlosti. Nižšie uvedený obrázok 3.3 reflektuje tok dát z jednej roviny do druhej a tiež medzi dvoma susednými zariadeniami. Rovina management plane zodpovedná za konfiguráciu zariadenia a nastavuje rovina control plane, v tomto prípade smerovanie z zariadení. Po výmene informácií so susednými smerovačmi sa vytvoria príslušné tabuľky a nakoniec smerovacia tabuľka, ktorá sa využíva pri rozhodovaní prepínania paketov v rovine data plane.



Obr. 3.3: Rozdelenie rovín v smerovači, tok informácií v jeho vnútri a medzi susednými smerovačmi [9]

3.4 Prevádzkové a bezpečnostné postupy

Riadenie a zneužitie prístupu k manažmentu zariadenia

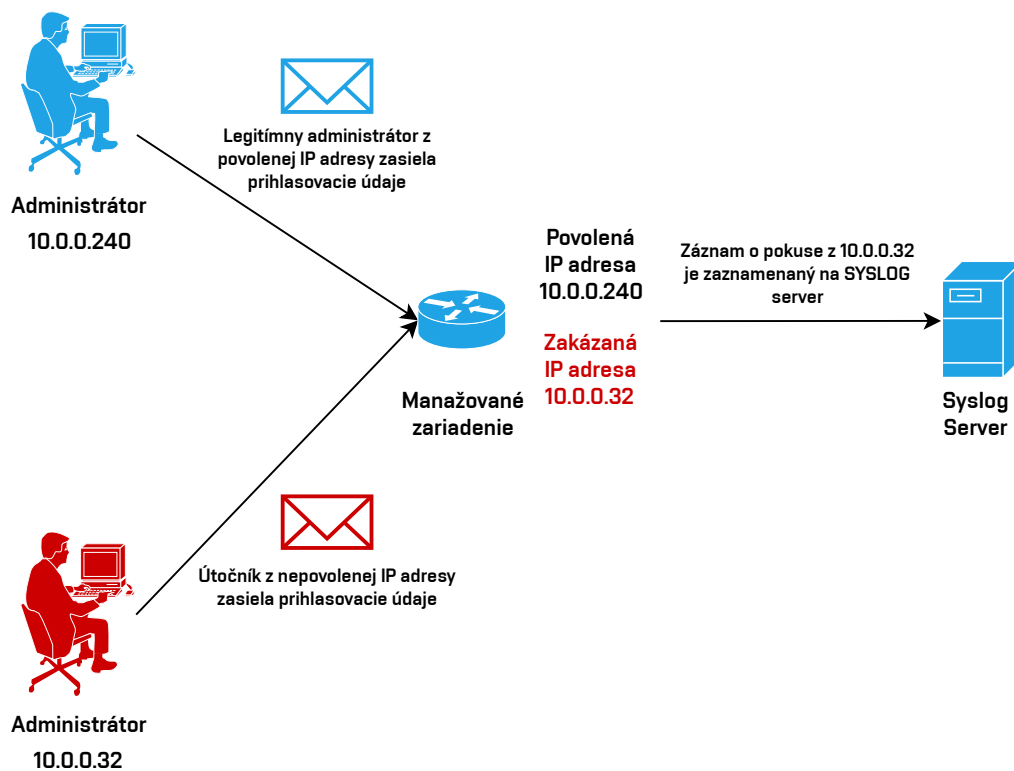
Kritickým miestom často absentujúcim zabezpečenie je prístup ku konfigurácii zariadenia. Typickým príkladom je využitie protokolu Telnet, ktorý nešifruje spojenie a je teda ľahko odpočúvateľný. Preto sa odporúča využívať protokol SSH, naviac je dobré využiť bezpečnú verziu 2 s rozumnou dĺžkou kľúča odpovedajúcou aktuálnym odporúčaniam [10] [11]. Jedným z opatrení na zabezpečenie SSH prístupu je zmena portu, na ktorom obvykle počúva z dôvodu, že útočník skúša periodicky útoky hrubou silou na *Transmission Control Protocol* (TCP) port 22. Alternatívou na zabezpečenie SSH prístupu môže byť port knocking, ktorý na základe autorizácie dynamicky povolí záznam v ACL k portu, na ktorom počúva SSH.

Pri pokusoch o prihlásenie sa často využíva hádanie hesiel, preto je dobré určiť maximálny počet neúspešných pokusov a definovať čas po ktorý bude prihlásenie zablokované.

Riadenie prístupu k manažmentu zariadení by malo byť výhradne z obmedzeného rozsahu staníc administrátorov, na to poslúžia obmedzenia pomocou ACL, aby neprišlo k nechcenému prihláseniu alebo útoku DoS z nechcených klientských staníc. Je tiež dobré zaznamenávať neúspešné ale aj úspešné prihlásenia do manažmentu zariadenia.

V prípade konfigurácie viacerými administrátormi naraz môže vzniknúť konflikt, a preto je dobré zabezpečiť, aby v jednom okamihu mohol zmeny vykonávať iba jeden administrátor. Problémom môžu byť aj dlhé aktívne pripojenie k manažmentu zariadenia, ktoré môže byť zneužitie pri odblokovanom počítači administrátora.

Pri pokuse o prihlásenie alebo zmene nastavení je dobré informovať oznámením alebo správou potenciálneho útočníka s následkami, ktoré mu hrozia v prípade zneužitia zariadenia [10].

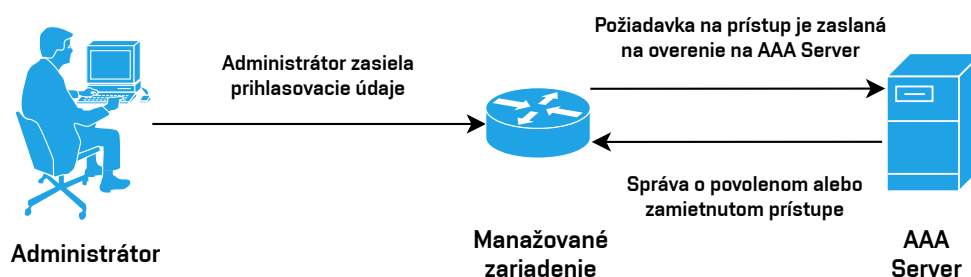


Obr. 3.4: Prihlasovanie k manažmentu zariadenia z povolených IP adries a logovanie pokusov z nepovolených IP adries

Ďalšou obranou proti nechcenému prístupu na sieťové prvky je vytvorenie lokálnych účtov, ktoré budú použité na prihlasovanie a pri zmenách konfigurácie. Bez znalosti kombinácií mena a hesla by nemalo byť umožnené zmeniť nastavenia zariadenia.

Riadenie prístupu pomocou AAA

Najlepším riešením pre riadenie prístupu k manažmentu zariadenia a účtovaniu sú protokoly spadajúce do skupiny AAA. Patria sem protokoly Radius, TACACS+ alebo Kerberos. Tieto protokoly umožňujú okrem riadenia prihlásení administrátorov tak tiež špecifikovať príkazy konfigurácie, ktoré budú jednotlivcom povolené a tiež zaznamenávať zmeny jednotlivých administrátorov v konfigurácií, ktoré učinili a naviac aj kedy boli na zariadení prihlásení. Zároveň je treba určiť aj mechanizmus prihlásenia pri výpadku autentizačného serveru, teda napríklad nejaké záložné lokálne konto.



Obr. 3.5: Overenie prihlásenia k manažmentu zariadenia pomocou AAA serveru

Filtrovanie prevádzky

Filtrovanie prevádzky môže prebiehať pomocou ACL, teda súborom pravidiel na vrstve L3 a L4, ktoré povoľujú alebo zakazujú komunikáciu. Jedným z dobrých praktík je filtrovať pakety so zdrojovou adresou privátnych alebo špeciálnych adries v smere do vnútornej siete z internetu [5]. Rozsahy týchto IP adries sú definované v RFC 6890 [12] a v RFC 8190 [13]. Administrátori často zabúdajú pri implementácii IPv6, že aj tento protokol má špeciálne adresy, ktoré nemôžu byť zdrojové, ak paket prichádza z internetu. Špeciálne IPv6 adresy sú definované v RFC 5156 [14] a aj vo vyššie spomenutých RFC. V prípade použitia týchto špeciálnych adries ako zdrojových sa jedná o útok typu IP spoofing.

IP Options

Protokol IPv4 umožňuje pomocou poľa Options vynútenie smerovania na základe zdrojovej adresy a definovanie cesty paketu, ale aj mnohé iné funkcionality. Toto pole

nie je však používané a odporúča sa zahadzovať pakety obsahujúce pole Options [7]. Jedným z dôvodov je preťaženie smerovača, keďže každý paket sa musí spracovávať v procesore a nemôže byť akcelerovaný v špeciálnych obvodoch a tým urýchléné jeho preposlanie.

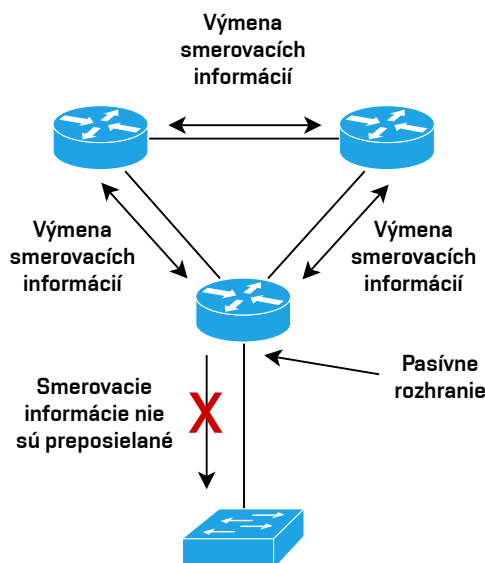
IPv6 rozšírené hlavičky

Protokol IPv6 nemá pole Options, ale tzv. Next Header. Problémom s rozšírenou hlavičkou sa zaoberá v článkoch Martin Grégr a Tomáš Podermaňski [15] [16]. V tomto poli môže byť definovaný protokol vyššej vrstvy, napríklad TCP, ale aj rozšírená hlavička, preto má smerovač problém často rozpoznať, ktoré z týchto dvoch sa nachádza v políčku a ako sa má zachovať, či ide o rozšírenú hlavičku alebo nový protokol. To čo nastane s paketom a ako sa zariadenie zachová závisí od implementácie softvéru v smerovači. Ten sa môže reštartovať, hlavičku preskočiť, zahodiť paket alebo na základe nesprávneho spracovania preskočiť pravidlo zahodenia paketu. Z týchto dôvodov a hlavne preskočením filtrácie sú rozširujúce hlavičky nebezpečné. Administrátor sa môže k nim stavať viacerými spôsobmi, a to zahodením každého paketu s rozširujúcou hlavičkou, zahodenie paketu s neznámou hlavičkou alebo ignorovanie tohto problému. Keďže niektoré rozširujúce hlavičky sú potrebné a používané, tak je dobrou zásadou odfiltrovať práve tie, ktoré zariadenie nevie rozpoznať. V súvislosti s rozšírenými hlavičkami sa zneužíva aj fragmentácia, a to takým spôsobom, že paket sa rozdelí na malé časti a rozšírená hlavička je až v poslednom fragmentovanom pakete. Predpokladá sa, že zariadenie si nevie znovu poskladať a spracovať takto zretazenú hlavičku a preto dôjde k obídeniu filtrovacích pravidiel. Touto problematikou sa zaoberá RFC 7112, ktoré definuje, aby rozšírená hlavička bola už v prvom pakete a tým bolo možné rozpoznať o akú rozšírenú hlavičku ide. Plošné zakázanie rozširujúcich hlavičiek nie je dobré, keďže sa využíva aj pre IPSec.

Smerovacie protokoly

Používaním dynamických smerovacích protokolov prichádza sieť o určitú časť bezpečnosti a to vysielaním informácií o pripojených a naučených sieťach a cestách, ktoré môže útočník odchytať. K tomu sa ešte môže pridať vloženie falošnej informácie a teda zaistenie smerovania cez útočníka. Našťastie obrana proti týmto útokom existuje, aj keď nie je vždy ideálna. V prípade vloženia informácie alebo cesty do správ, ktoré si vymieňajú dynamické smerovacie protokoly je možnou obranou autentizácia správ poslaných medzi smerovačmi [3] [7] [10]. Pri zasielaní sa používa hash hesla a to sa pri prijatí druhým smerovačom porovná s vopred definovaným. Na obrázku 3.6 je vidno, že informácie dynamického smerovacieho protokolu sú

zastavené na pasívnom rozhraní [17], a teda užívatelia alebo útočník nemá možnosť sa tieto údaje dozvedieť.



Obr. 3.6: Blokovanie správ dynamického smerovacieho protokolu na pasívne rozhranie

Source Routing

Bezpečnostnou hrozbou môže byť aj smerovanie na základe zdrojovej adresy, pri ktorej si zdroj určí cestu, ktorou bude paket prechádzať namiesto aby túto skutočnosť prenechal na rozhodnutí smerovačov po ceste k cieľu [10]. Táto funkcia využíva pole `IP Options`, ktoré býva však často ignorované prípadne pakety s týmto polom zahadzované z bezpečnostných dôvodov. Existujú dva módy, a to `Strict` a `Loose`, v prvom prípade musí paket prejsť všetkými definovanými bodmi a žiadnym iným. Naopak mód `Loose` definuje uzly, ktoré je potreba navštíviť, no zároveň môžu byť navštívené aj iné uzly po ceste.

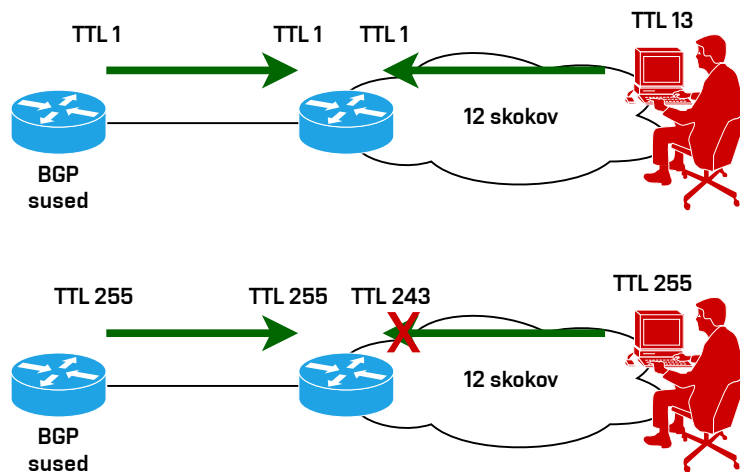
Unicast reverse path forwarding

Podvrhnutie IP adresy, tzv. IP spoofing je jedným z útokov, ktorým musia smerovače čeliť. Dá sa mu zbrániť pomocou *Unicast Reverse Path Forwarding* (uRPF) [5], ktorý funguje buď v `Strict` alebo `Loose` móde a zisťuje prítomnosť zdrojovej IP adresy. Ako už názov napovedá, tak mód `Strict` je prísnejší, pretože zahadzuje pakety, ktorej zdrojová adresa sa nenachádza v smerovacej tabuľke a zároveň testuje či zdrojová adresa je dosiahnuteľná cez rozhranie, na ktorom bol paket prijatý. Tento

mód je preto nevhodný pri asymetrickom smerovaní. Mód Loose testuje prítomnosť zdrojovej adresy iba v smerovacej tabuľke.

BGP TTL Security

Protokol *Border Gateway Protocol* (BGP) okrem autentizácie obsahuje aj ďalšiu ochranu a to *Time To Live* (TTL) security [18]. Pri tomto prístupe sa porovnáva hodnota poľa TTL v pakete, ktorý dorazí do smerovača a známy počet skokov, ktorý sa nakonfiguruje medzi našim smerovačom a zdrojom. Mohlo by sa zdať, že priamo pripojené siete, teda susedné autonómne systémy týmto problémom netrpia, no pole TTL sa dá zmeniť tak, aby po príchode na smerovač obete malo toto pole hodnotu 1, čo je predvolené TTL, ktoré zasiela BGP, viď obrázok 3.7. Z tohto dôvodu sa používa obrátená forma kontroly, a to testovanie voči maximálnej hodnote TTL, čo je hodnota 255. To znamená, že všetky pakety od priamo pripojených BGP susedov budú mať po príchode na náš smerovač hodnotu TTL 255, tie ktoré to nebudú spĺňať sú brané ako nelegitímne pakety, viď 3.7. Treba dodať, že v prípade že routery nie sú priamo pripojené, tak je možné použiť aj definovanie vzdialenosti medzi smerovačmi, teda počet skokov, aby susedný smerovač dostal BGP správu. Bezpečnejšie je však použiť TTL security, tak že sa od čísla 255 odpočíta počet skokov medzi dvoma autonómnymi systémami a voči tejto hodnote sa bude robiť kontrola.



Obr. 3.7: Porovnanie prístupov TTL security, kde sa v prvom prípade používa implicitná hodnota 1 na porovnanie TTL a v druhom prípade maximálna hodnota TTL [18]

Identifikácia zariadení, pravidiel a nastavení

K lepšej identifikácii je dobrým pravidlom každé sieťové zariadenie vhodne pomenovať kombináciou typu zariadenie, vrstvy hierarchického modelu, na ktorej operuje a prípadne umiestnenia v racku, napríklad `sw01-dist-rack1`. V súvislosti s týmto nastavením sa často nastavuje aj doména, v ktorej je zariadenie umiestnené. Tieto dve prerokvity potom umožňujú aj vzdialenú správu zariadenia a prístup cez SSH [10].

Dôležitým prvkom sú komentáre k pravidlám v ACL, ktoré by mali nielen identifikovať, čo presne dané pravidlo povoľuje a zakazuje, ale aj identifikovať požiadavom, na základe ktorého bolo pravidlo vytvorené.

Komentáre s popisom je dobré pridávať aj na rozhrania sieťových zariadení, napríklad s popisom, k akému zariadeniu dané rozhranie vedie. Posledným, ale nemenej dôležitým je pomenovanie VLAN pre ich ľahšiu identifikáciu.

Šifrovanie hesiel

Pri úniku konfigurácií môže dôjsť k odhaleniu hesiel uložených v nich, preto by mali byť v konfiguračnom súbore všetky heslá zahašované pomocou čo najpokročilejších hašovacích funkcií, ktoré dané zariadenie podporuje [10].

Logovanie

Záznam činnosti zariadenia patrí k základným prvkom monitorovania sieťovej infraštruktúry spolu s notifikovaním o vzniknutých incidentoch. Na tieto účely sa používa prevažne dva protokoly, a to SNMP a Syslog.

Protokol SNMP využíva databázu MIB buď štandardizovanú, alebo rozšírenú daným výrobcom zariadenia. Jednotlivé monitorované objekty sú v tejto databáze organizované v stromovej štruktúre. V súčasnosti sa využívajú prevažne SNMP verzie 2c a 3. Je vysoko odporúčané využívať verziu 3, ktorá zabezpečuje ako integritu, tak aj dôvernú a autentizáciu [10] [19]. Protokol SNMP umožňuje pomocou jednotlivých objektov meniť nastavenia zariadení, túto funkciu je však dobré vypnúť a povoliť iba čítanie objektov z presne definovaných IP adries pomocou ACL a asynchrónne správy TRAP.

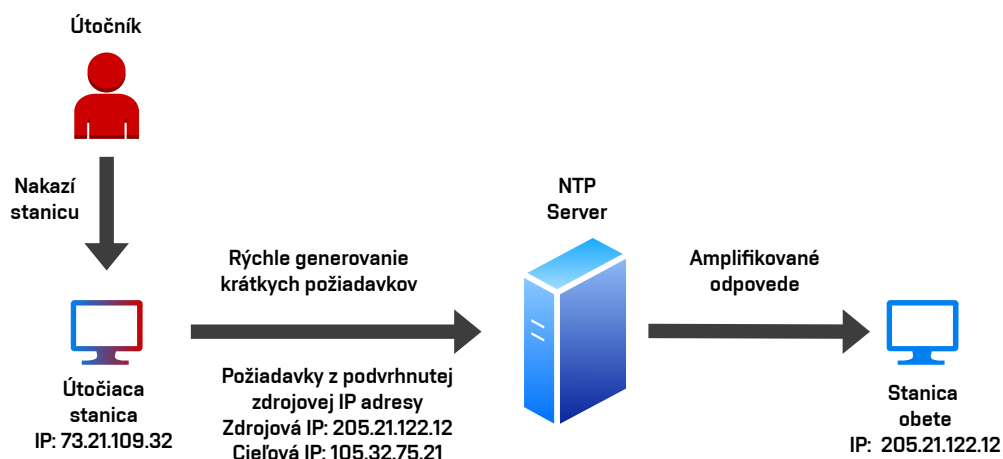
Druhou možnosťou monitorovania a notifikovania o incidentoch je protokol Syslog. Typicky sa nastavuje Syslog server, ktorý zbiera správy z viacerých zariadení, ktoré môžu byť následne spracovávané špeciálnymi programami a vizualizované v dohľadových centrách. Protokol Syslog pozná 8 úrovní dôležitosti (severity), pričom čím nižšie číslo dôležitosti, tým ide o závažnejší problém. Pri výpadku Syslog serveru je nutné záznamy ponechať na zariadení a preto mať dostatočné množstvo pamäte

[7] [20]. V niektorých prípadoch môžu zariadenia vygenerovať väčšie množstvo správ, ktoré majú rovnaký čas a z tohto dôvodu by mali mať jednotlivé správy s rovnakým časom vzniku jednoznačné sekvenčné číslo, aby bolo možné zistiť postupnosť, v akom vznikli incidenty, napríklad zmeny v susedstvách dynamických smerovacích protokoloch.

Vela útokov mieri práve na protokol SNMP, a preto ho mnohí odporúčajú vypínať [10], na druhej strane protokol Syslog nezabezpečuje žiadnu časť z triády CIA.

Synchronizácia času

Správny a aktuálny čas je dôležitý hlavne pre správne fungovanie certifikátov a protokolu Syslog. V prípade protokolu Syslog zabezpečuje jednoznačnú identifikáciu incidentu v správnom čase a teda lepšiu dohľadateľnosť a určenie vzniku problému. Keďže tento protokol využíva *User Datagram Protocol* (UDP), tak je náchylný na DDoS reflektívne amplifikačné útoky. Tento typ útoku využíva krátku správu zasielanú na NTP server s podvrhnutou zdrojovou IP adresou (IP Spoofing), na ktorú budú zasielané odpovede s oveľa väčšou veľkosťou ako boli pôvodné správy na NTP server. Bohužiaľ obrana proti tomuto typu útoku je veľmi ťažká, poskytovatelia pripojenia k internetu sa s týmto neuhom väčšinou dokážu popasovať [21], v lokálnych sieťach môže pomôcť IP Snooping. Podľa Network Time Foundation [22], aktuálna verzia protokolu 4 nepodporuje šifrovanie správ, no poskytuje akú-takú bezpečnosť pre koncových NTP klientov pomocou MD5 a to autentizáciu NTP serveru a kontrolu integrity. Navyše protokol nepodporuje žiadnu distribúciu kľúčov. Protokol NTP verzie 4 podporuje aj asymetrickú kryptografiu pomocou Autokey, no podpora tohto riešenia je veľmi slabá [22], jedným z dôvodov je aj náročnosť výpočtov. NTP podporuje sťahovanie správ aj od klientov, toto je výhodné pri prerušení linky ku NTP serveru a na krížovú kontrolu času. Dôležitým nastavením je aj správne časové pásmo, ktoré je dobré zjednotiť naprieč všetkými spravovanými zariadeniami. V prípade roztrúsenia zariadení cez viacero časových pásiem je dobré využívať univerzálny čas UTC. Okrem protokolu NTP existuje niekoľko ďalších protokolov na synchronizáciu času, no sú menej používané. Príkladom je *Precision Time Protocol* (PTP), ktorý je vhodný do lokálnych sietí kvôli vysokej presnosti.



Obr. 3.8: Ilustrácia aplifikačného útoku cez nakazený počítač pomocou podvrhutej IP adresy [21]

Záloha a zabezpečenie konfigurácií

Konfigurácie zariadení a ich záloha sú veľmi dôležitým faktorom, ktorým sa treba zaoberať pri správe infraštruktúry. Pokiaľ sú prítomné aktuálne konfigurácie zariadení, tak pri výpadku hardware je možné ho vymeniť za nový a aplikovať fungujúcu konfiguráciu z poškodeného zariadenia zo zálohy. Zároveň by sa konfigurácia mala dostatočne zabezpečiť proti výmazu zo zariadenia a zálohovaného úložiska a dostatočne zabezpečiť [3]. Zabezpečenie je dôležité, aby nedošlo k úniku konfigurácie útočníkom a nepovolaným osobám a následnému zneužitiu. Záloha konfigurácií by sa mala robiť cez zabezpečený kanál najlepšie pomocou protokolov podporujúcich šifrovanie, napríklad *Secure Copy Protocol* (SCP) alebo *Secure File Transfer Protocol* (SFTP) a nie pomocou *Trivial File Transfer Protocol* (TFTP) [7]. Vhodná je aj prítomnosť záznamu zmien v konfigurácií v čase [3].

Správanie pri vysokom zaťažení

V priebehu prevádzky sa môže vyskytnúť kratší alebo aj dlhý časový okamih, kedy je zariadenie vysoko zaťažené a nevláda spracovávať požiadavky. Toto môže byť spôsobené útokom (D)DOS alebo nedostatočným dimenzovaním a zlou architektúrou siete. Aj napriek tomuto stavu by však malo byť zariadenie schopné odosielať chybové správy a notifikovať o problémoch. Zároveň by mali byť nastavené prahové hodnoty, ktoré budú indikovať stav, že môže dôjsť k nadmernému vyťaženiu procesoru, pamäti alebo linky či už pomocou Syslog správ alebo protokolu SNMP [20] [7].

Monitorovanie výkonu siete

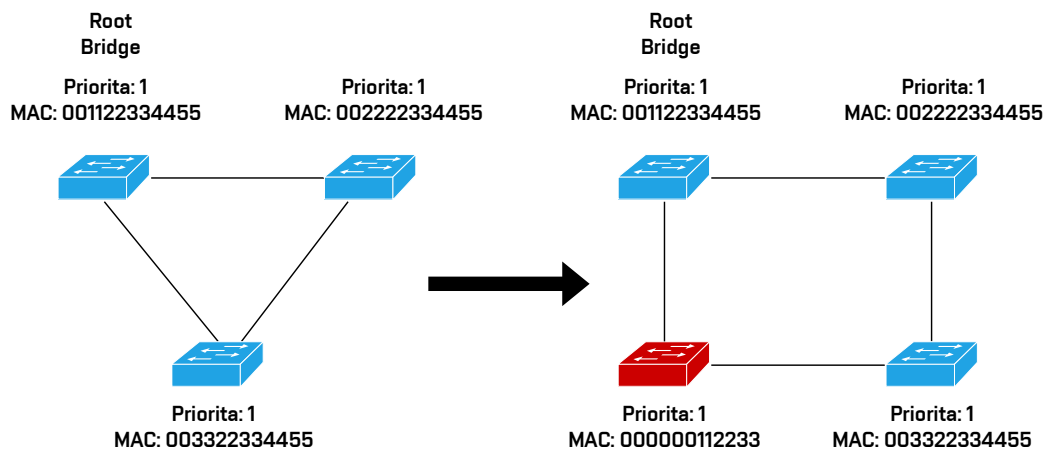
Monitorovanie siete nie je len o chybových a operačných správach zariadení, ale aj o prevádzke, ktorá v sieti prebieha. Toto monitorovanie prevádzky musí byť vykonávané často z legislatívnych dôvodov a aplikuje sa u poskytovateľov pripojenia. Monitorovanie prevádzky sa však vykonáva aj v lokálnych sieťach, napríklad zrkadlením portov [7] na analýzu útokov pre IDS alebo pre štatistické informácie a informácie o zaťažení pomocou protokolov sFlow a NetFlow.

Problémy vrstvy L2

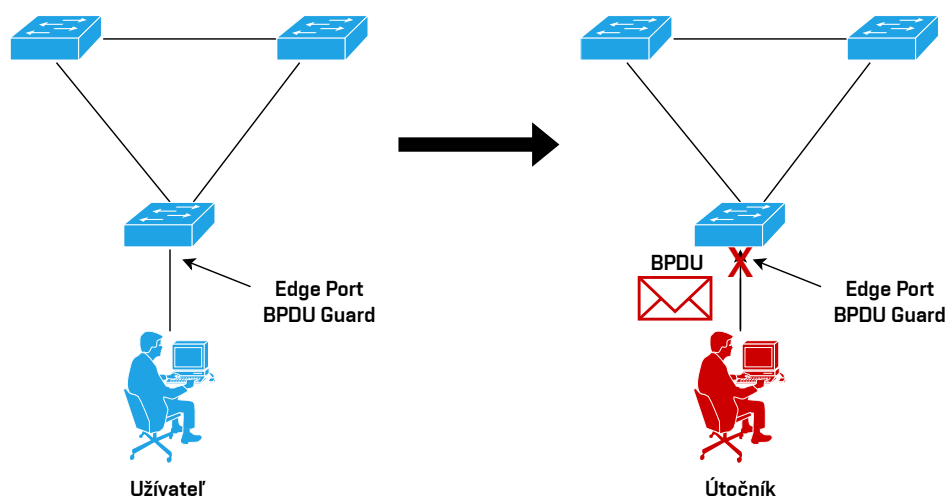
Prístupová vrstva hierarchického modelu alebo vrstva L2 modelu ISO/OSI je časť siete, do ktorej sa pripájajú zväčša koncové zariadenia. Vzniká tu preto mnoho problémov či už bezpečnostných alebo prevádzkových, na ktoré je nutné myslieť.

Spanning Tree Protocol

Protokolom pracujúcim na vrstve L2 je *Spanning Tree Protocol* (STP), zaisťujúci bezslučkovú topológiu aj v prípade cyklického zapojenia prepínačov z dôvodu redundancie [8]. Existuje mnoho implementácií STP protokolu, každé však zabezpečuje logické vypnutie alebo zakázanie portu aj pri existujúcom fyzickom pripojení. Pre urýchlenie výpočtu kostry a konverencie siete sa vylučujú z výpočtu porty, na ktoré sú pripojené koncové zariadenia a teda nepredpokladá sa na týchto portoch pripojený prepínač. Tento fakt môže na druhej strane spôsobiť slučky v prípade zapojenie prepínača do takéhoto portu. Z tohto dôvodu existuje tzv. BPDU Guard [8], čo je ochrana, kedy pri prijatí rámca s BPDU označeným červeno na obrázku 3.10 na port vyradený z výpočtu kostry grafu je port zablokovaný a neumožňuje preposielať rámce. Ďalšou ochranou je Root Guard [2], ktorý zabráňuje novo pripojeným prepínačom prebrať rolu hlavného prepínača pre danú podsieť alebo VLAN. Jeho úžitok zobrazuje nasledujúci obrázok 3.9, kde po pripojení nedovoleného prepínača označeného červeno príde nepríde k zvoleniu nového Root Bridge kvôli ochrane Root Guard. Existuje ešte ochrana Loop Guard [2], ktorá zabezpečuje, že pri poruche a jednosmernej komunikácii medzi prepínačmi nedôjde k vytvoreniu slučiek. Táto ochrana je však výhradne u zariadení od spoločnosti Cisco.



Obr. 3.9: Zabránenie prebratia role Root Bridge pomocou Root Guard, kde pri pripojení nedovoleného prepínača (označený červeno) s nižšou MAC adresou nebude prepínač zvolený za Root Bridge

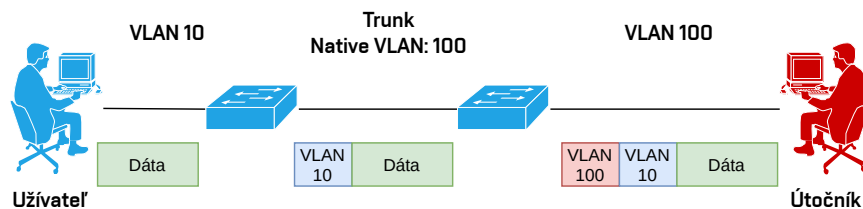


Obr. 3.10: Zabránenie vyhlásenie koncového portu ako portu k prepínaču pomocou BPDU Guard, kde po prijatí rámca s BPDU označeným červeno, príde k zablokovaní portu

Bezpečnosť VLAN

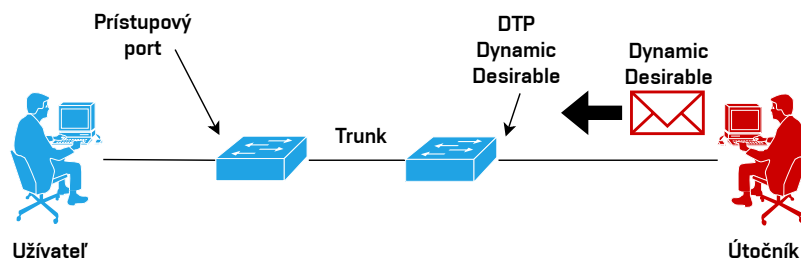
Referenčná príručka bezpečnosti [20] definuje nižšie popísané útoky na vrstve L2 a obranu na ne. V predvolenom stave sú zväčša všetky porty v jednej VLAN, ktorá je implicitne povolená na všetkých trunk portoch respektíve portoch, kadiaľ prechádza tagovaná prevádzka. Preto je dobré všetky aj nepoužívané porty odobrať z predvolenej VLAN a nepripojené porty prideliť nikam nesmerovanej VLAN. Taktiež by

sa predvolená VLAN nemala používať na tagovanú prevádzku a to aj z dôvodu, že pri zabudnutí odstránenia prístupových portov z predvolenej VLAN môže dôjsť k útokom VLAN hopping za pomoci Double tagging. Na tagovaných trunk portoch by mala byť povolená prevádzka iba takých VLAN, ktoré sú potrebné a zakázaná pre VLAN, do ktorej sú umiestnené nevyužívané porty. Útoku double tagging sa dá zabrániť špecifikovaním VLAN na prístupových portoch a definovaním separátnej VLAN na tagovaných trunk portoch.



Obr. 3.11: Útok Double tagging, pri ktorom útočník zasiela rámec s dvoma VLAN ID, kde prvé bude odstránené na prvým prepínačom, keďže trunk má tagovanú prevádzku na VLAN 100, tak dôjde k preposlaniu rámcu až k obeti [23]

Predstieranie, že koncové zariadenie je prepínač sa dá zneužitím protokolu *Dynamic Trunking Protocol* (DTP) [20]. Pri tomto útoku s názvom Switch spoofing, prepínač aktívne alebo pasívne čaká na odpoveď, že na druhej strane prístupového portu je prepínač. Ak mu dôjde od koncového zariadenia takáto správa, tak sa prepne pôvodne prístupový port na port typu trunk. Z tohto dôvodu je dobrou zásadou tento protokol nevyužívať a porty konfigurovať ručne ako prístupové alebo trunk.



Obr. 3.12: Útok Switch spoofing pomocou protokolu DTP, prepínač aktívne čaká na správu DTP alebo stav portu trunk, útočník zasiela správu (označenú červenou) žiadajúcu o vytvorenie trunk portu, trunk bude nakoniec vytvorený

Istou formou zabezpečenia je aj explicitne zakázať nepoužívané prístupové porty, aby ich nebolo možné zneužiť, keďže často pri neaktívnych portoch absentujú rôzne

bezpečnostné nastavenia, z dôvodu, že pri prvotnom nasadení zariadenia sa nevyužívali.

Proprietárny protokol *Virtual Trunking Protocol* (VTP) a štandardizovaný *Multiple VLAN Registration Protocol* (MVRP) a ich predchodcovia umožňujú distribúciu a synchronizáciu VLAN informácií na skupinu prepínačov [2]. Na jednej strane tieto protokoly uľahčujú administráciu, no pri neopatrnosti môže pri zapojení nového zariadenia do siete prísť k výmazu VLAN informácií na všetkých pôvodných prepínačoch. Preto je dobré tento protokol používať iba pri prvotnom nasadení a vytváraní siete. V prípade nutnosti používania tohto protokolu je dobré zabezpečiť správy posielané medzi prepínačmi, aby nedošlo k ich manipulácií po ceste. Tak tiež je v prípade použitia týchto protokolov výhodné zapnúť funkciu pruning, ktorá umožňuje zasielať broadcast iba na tie prepínače, ktoré majú porty v danej VLAN.

First Hop Security

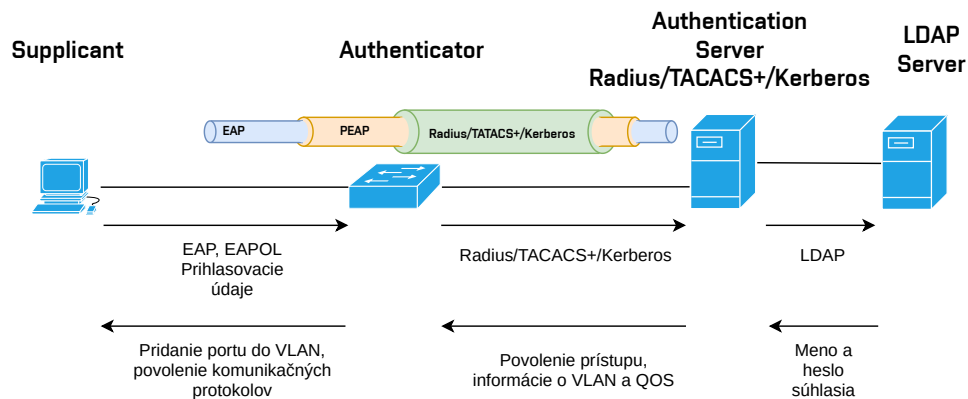
First Hop Security je označenie pre niekoľko prístupov k zabezpečeniu koncových staníc a mitigáciu rôznych zneužití a podvrhnutí. Treba povedať, že protokoly IPv4 a IPv6 sa mierne odlišujú vzhľadom ku rozdielnemu postoju k pridelovaniu adries [24].

Port Security

Prístupové porty, ktoré sa využívajú na pripojenie klientských staníc zväčša absentujú akoukoľvek identifikáciou pripojeného zariadenia. Najjednoduchším spôsobom je definovanie maximálne jednej povolenej MAC adresy na porte. Tento typ obrany naviac zamedzí útoku MAC flooding, kde dochádza k zaplaveniu portu náhodnými MAC adresami za účelom preťažiť CAM tabuľku prepínača a donútiť ho posilať všetko ako broadcast. Pri prekročení limitu počtu adries na port by mal byť notifikovaný administrátor a port by mal pozastaviť preposielanie rámcov.

Napriek vyššie zmienenému opatreniu, nič nebráni útočníkovi zmeniť MAC adresu na útočiacom zariadení, aby mu bol povolený prístup do lokálnej siete, tento typ zneužitia sa volá MAC spoofing. Naviac takéto nastavenie zamedzí využívanie prípojky legitímnym užívateľom. Z tohto dôvodu vznikol štandard 802.1x, ktorý definuje akým spôsobom bude užívateľ respektíve koncová stanica na porte autentizovaná [2]. Tento štandard využíva protokoly *Extensible Authentication Protocol* (EAP), *Protected Extensible Authentication Protocol* (PEAP), *Extensible Authentication Protocol over LAN* (EAPoL), RADIUS, TACACS+, Kerberos a definuje tri role pre zariadenia podieľajúce sa na autentizácii. Prvým typom zariadenia je

Supplicant, čo je koncové zariadenie, ktoré zasiela prístupové údaje na zariadenie Authenticator, ktorým je zväčša prepínač. Na porte prepínača, na ktorý je pripojený Supplicant sú bez overenia povolené len protokoly EAP, EAPOL prípadne CDP/LLDP a je umiestnený do izolovanej VLAN. Po úspešnom overení pomocou autentizačného serveru, ktorý porovná preposlané prihlasovacie údaje od prepínača s autentizačným serverom, budú na porte povolené všetky potrebné protokoly a koncové zariadenie bude v náležitej VLAN. Nižšie uvedený zjednodušený obrázok 3.13 ilustruje komunikáciu koncovkej stanice s prepínačom a autentizačným serverom.



Obr. 3.13: Zjednodušená komunikácia koncovkej stanice s prepínačom, ktorý preposiela prihlasovacie údaje serveru na overenie na následné povolenie komunikácie na porte [2]

DHCP Snooping

Protokol IPv4 využíva centralizované pridelenie IP adries za pomoci DHCP serveru. Výhodou je, že všetky pridelené adresy sú dostupné na jednom mieste, no zároveň toto riešenie porušuje vrstvomý model sietí, keďže aplikačný protokol DHCP konfiguruje protokol nižšej vrstvy. Problém v prípade útoku DHCP spoofing Man-in-the-middle je, že v sieti môže byť viacero DHCP serverov a ten, ktorý odpovie rýchlejšie, teda útočníkov môže prinútiť koncovú stanicu, aby si vybrala adresu ponúkanú ním. To znamená, že môže napríklad všetku sieťovú prevádzku z koncového zariadenia smerovať cez bod siete, ktorý útočníkovi vyhovuje. Obranou na tento útok je DHCP snooping [2] [7], kedy sa definujú porty, ktoré sú dôveryhodné a teda, môžeme z nich prijímať správy DHCP Offer a DHCP Acknowledge. Prepínač si následne vytvorí mapovanie IP adresy pridelennej DHCP serverom, MAC adresy koncového zariadenia, VLAN a portu, na ktorom je zariadenie pripojené. DHCP Snooping tiež zabraňuje vyčerpaniu adries pridelených pomocou DHCP serveru, kde útočník posielal správy DHCP Request s podvrhnutými MAC adresami, aby vyčerpal rozsah,

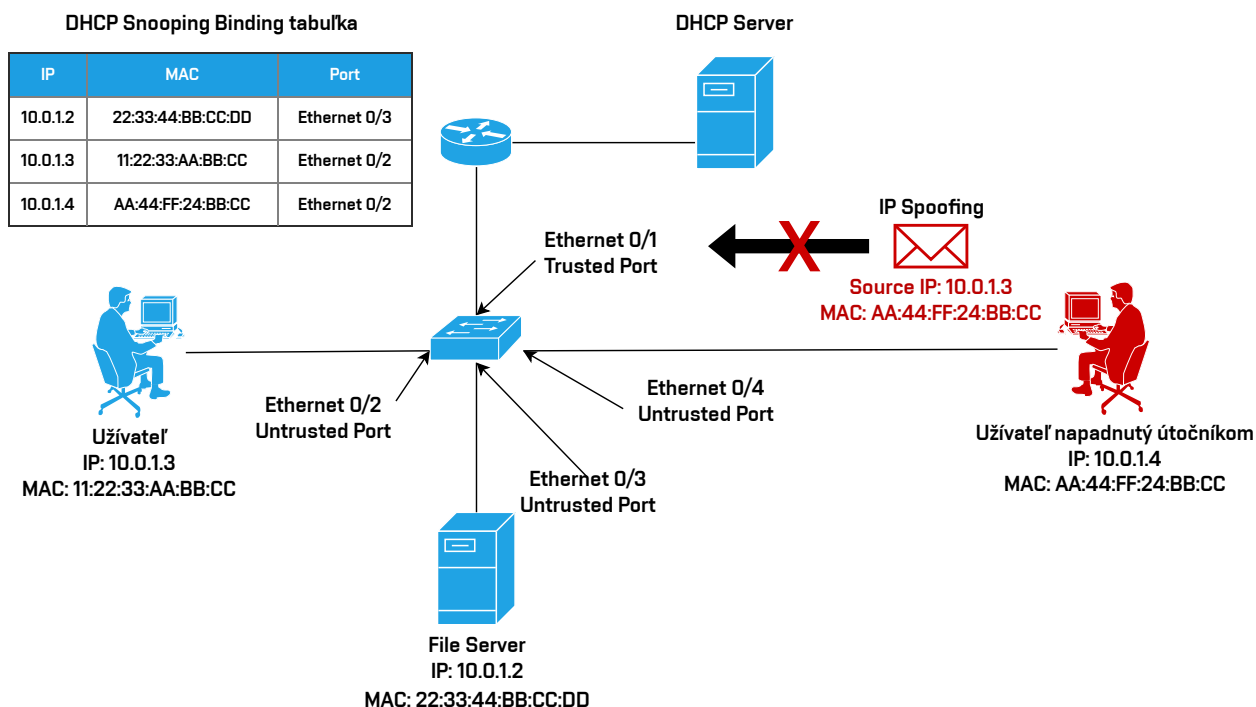
ktorý sa prideluje klientom.

Dynamic ARP Inspection

Protokol ARP býva zneužitý na útok ARP spoofing. Pri tomto útoku útočník na dotaz užívateľa, v ktorom sa pýta, akú MAC adresu má zariadenie, ku ktorému pozná IP adresu, odpovie svojou MAC adresou alebo MAC adresou uzla v sieti, cez ktorý má prechádzať komunikácia. Týmto zabezpečí, že dáta bude možné odchytať na stanici, ku ktorej má prístup. Obranou proti tomuto zneužitiu je Dynamic ARP Inspection [3], ktorá porovnáva údaje získané z tabuľky vybudovanej pomocou DHCP Snoopingu. Pokiaľ ARP odpoveď z portu neodpovedá naučenej informácii, tak je paket ARP odpovedi zahodený. Preto je nutnosťou pre využitie tejto obrany mať zapnutú funkciu DHCP snooping.

IP Source Guard

Ďalším častým útokom na prístupovej vrstve je IP spoofing, a teda používanie a zneužitie IP adresy, ktorá koncovému zariadeniu nepatrí. Útočník pomocou tohto útoku môže zahltiť stanicu tak, že ako zdrojovú IP adresu paketu uvedie IP adresu obeti a predpokladá, že odpoveď na tento paket už nebude doručená jemu, ale obeti. Mitigácia tohto útoku je možná za pomoci IP Source Guard [7], ktorá v každom odchádzajúcom pakete skontroluje, či IP adresa vysielajúcej stanice súhlasí so zdrojovou IP adresou. Nutnou prerekvizitou je vybudovanie tabuľky za pomoci DHCP snoopingu.



Obr. 3.14: Využitie DHCP Snoopingu pre IP Source Guard, pri ktorom útočník napadne užívateľov počítač a snaží sa s podvrhnutou IP adresou zaslať paket, ten nezodpovedá mapovaniu v tabuľke na prepínači a bude zahodený

Pridelovanie adries v IPv6

Protokol IPv6 používa odlišný prístup k prideleniu IPv6 adries, a teda nie všetky mitigácie útokov z protokolu IPv4 sú realizovateľné. V prvom rade systém pridelenie IPv6 adries nie je povinne centralizovaný a na konfiguráciu adries sa používa protokol *Internet Control Message Protocol version 6* (ICMPv6). Je možné použiť aj DHCPv6 server, no ten nie je v štandarde definovaný ako povinný, a preto ho niektoré systémy vôbec nepodporujú. Zariadenie dostane buď od smerovača, alebo si od neho vyžiada správu Router Advertisement. V nej dostane prefix siete, prípadne ďalšie informácie a následne si spodných 64 bitov do adresy zvolí náhodne alebo si ich odvodí z MAC adresy. Keďže nie je pridelenie centralizované a môže dôjsť k duplicite adries je treba zistiť ICMPv6 správou či zvolená adresa nie je v sieti už používaná. Práve v tomto spočíva prvý útok, kedy na správu overujúcu použitie adresy v sieti reaguje útočník, že ju má pridelenú práve on [25]. Zariadenie si vygeneruje novú adresu a pokus opakuje, útočník mu znova odpovie rovnako a teda mu odopiera prístup a znemožní mu využívať sieť. Kontrola prítomnosti adresy sa vykonáva aj v prípade využitia DHCPv6 serveru, takže ani jeho prítomnosť tento problém neodstráni.

Zabezpečenie ohlásení susedov

Protokol ICMPv6 a správa Neighbor Solicitation sa v IPv6 používa namiesto protokolu ARP pre zistenie MAC adresy, teda z toho plynú podobné problémy ako pri IPv4. Čiastočná mitigácia problému je pomocou ND Inspection, no ten využíva princíp „Trust on first use“ alebo „First come first serve“, teda do tabuľky podobnej DHCP Snooping sa zapíše hodnota prvej prihlásenej stanice [27] [28]. Tým môže útočník taktiež odstaviť užívateľa od pripojenia a zamedziť kontrolu duplicity adries, pokiaľ si svoje zariadenie prihlási ako prvé. Druhou možnosťou je DHCPv6 snooping, no ten je komplikované realizovať v prípade staníc s rôznymi systémami kvôli nekompatibilitate tohto protokolu naprieč operačnými systémami. Riešením by bol protokol *Secure Neighbor Discovery* (SEND), no ten sa kvôli komplikovanosti a problémom s licenciami nepoužíva [26].

Falošný smerovač

Oznámenie smerovača môže byť podvrhnuté falošným smerovačom – Rogue RA alebo koncové zariadenie môže byť zaplavené falošnými prefixmi – RA Flood [27] [28]. Z tohto dôvodu je nutné používať obranu RA Guard, ktorá definuje na ktorom rozhraní prepínača je pripojený smerovač, ktorý zasiela správy Router Advertisement, teda prefixy siete a ostatné potrebné informácie. Je to obdoba trust portu u DHCP snooping. Navyše je nutné zabezpečiť, aby ohlásenie smerovača a suseda nebolo fragmentované, tak ako hovorí RFC 6980 [29].

IPv6 Source Guard

Kontrola IPv6 source guard, ktorá zabraňuje podvrhnutiu IPv6 adries je funkčná iba v prípade prítomnosti DHCPv6/IPv6 snooping a ND inspection, čo ako bolo popísané vyššie môže spôsobiť aj odoprenie služby legitímnemu užívateľovi. Preto pri použití ND inspection a DHCPv6/IPv6 snooping je vhodné pre kritické zariadenia, napríklad servery vytvoriť na prepínačoch manuálny záznam MAC a IPv6 adresy a VLAN.

Vyčerpanie pamäte susedov

Problémom v IPv6 je aj vyčerpanie pamäte susedov, kedy sa do tejto pamäte dostávajú neexistujúce útočníkve adresy, alebo je v sieti pripojených veľa staníc s priveľa IPv6 adresami na každý uzol [30] [31]. Tento problém pramení vo fakte, že koncové zariadenia majú hneď niekoľko IPv6 adries. Pri útokoch z internetu na globálne adresy môžeme vyfiltrovať pomocou ACL rozsahy sietí, ktoré nie sú v lokálnej sieti pripojené, a tým zamedziť ich zapísaniu do tabuľky. V lokálnych sieťach sa môže

definovať maximálna doba, po ktorú bude IPv6 adresa v zariadení zaznamenaná alebo sa staticky definuje mapovanie IPv6 a MAC adresy.

Nároky IPv6 na prenosné zariadenia

V IPv6 sieťach dochádza k problému častej komunikácie pomocou ICMPv6 správ. Jedná sa hlavne o správy pre ohlásenie smerovača, ohlásenie susedov respektíve o multicast komunikáciu. Pri mobilných zariadeniach pracujúcich na batériu by mohlo dôjsť k častému zobúdzaniu kvôli prijímaniu týchto správ a jej následnému vyčerpaniu. Z tohto dôvodu existuje RA throttling, ktorá obmedzuje množstvo správ typu ohlásenie smerovača [32].

V sieťach s IPv6 konektivitou je viac než žiadúce dbať na monitorovanie, keďže všetky útoky nie je možné potlačiť.

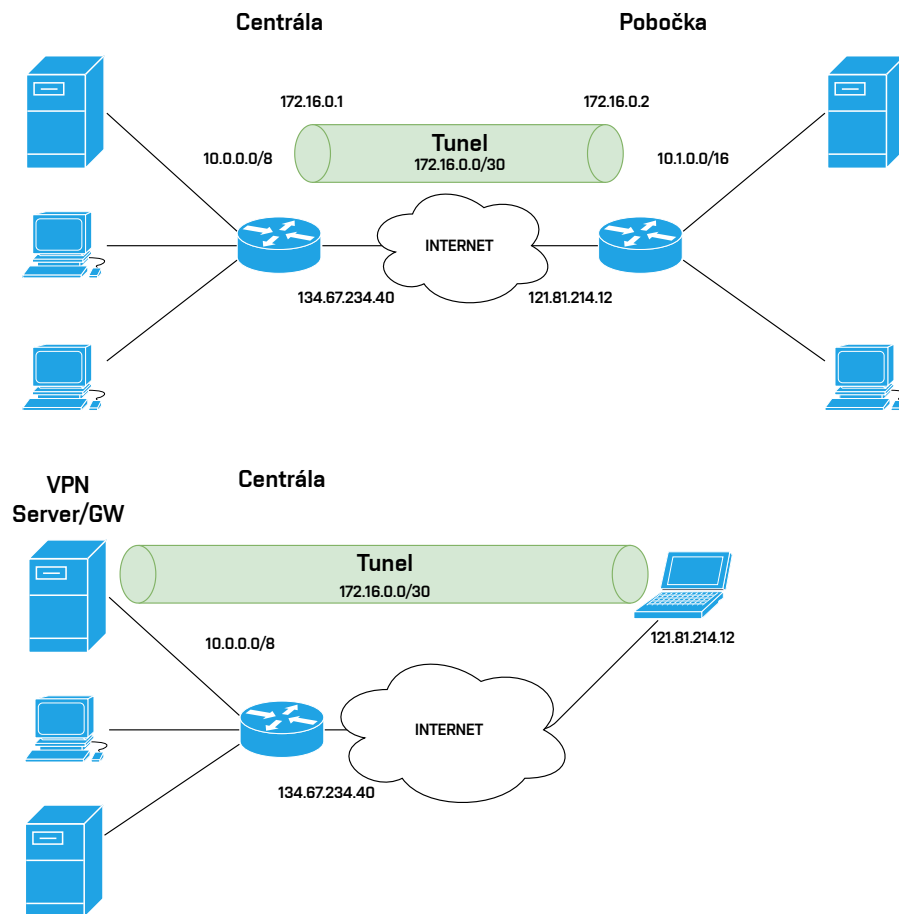
First Hop Redundancy Protocols

Protokoly na redundanciu brány štandardizovaný *Virtual Router Redundancy Protocol* (VRRP) a proprietárne *Hot Standby Redundancy Protocol* (HSRP) a *Gateway Load Balancing Protocol* (GLBP) umožňujú využívať jednu virtuálnu adresu pre východiu bránu na koncových zariadeniach a tým sú pre toto koncové zariadenie transparentné [8]. Navyše proprietárny protokol GLBP dokáže na ARP dotaz vracať ktorúkoľvek MAC adresu smerovača v skupine a tým rozkladať medzi ne záťaž. Všetky protokoly umožňujú autentizáciu správ zasielaných medzi sebou a tým istú úroveň bezpečnosti, aj keď nie úplne ideálnu.

Tunely a VPN

Virtual Private Network – *Virtuálna privátne sieť* (VPN) slúžia na vzdialené pripojenie zariadení, ktoré sú oddelené vonkajšou sieťou, internetom [8]. Pre pripojenie vzdialených zariadení sa využívajú tunely. Spravidla sa VPN rozdeľujú na dva druhy, a to site-to-site, kde je pobočka k centrále pripojená cez hraničné prvky siete pomocou permanentne vytvoreného tunelu. kde je vytvorené permanentné spojenie medzi hraničnými zariadeniami. Alebo druhou alternatívou je remote access VPN, kedy sa vytvára tunel na vyžiadanie a všetka sieťová prevádzka je môže byť smerovaná cez bod, ku ktorému sa stanica vzdialene pripája a zároveň je zariadeniu prístupná vnútorná sieť. Tieto tunely môžu byť šifrované, čo zabezpečuje dôvernosť a preto by mali byť preferovanou alternatívou. Dnes ešte stále používané protokoly *Point-to-Point Tunneling Protocol* (PPTP), *Layer 2 Tunneling Protocol* (L2TP) nie

sú v dnešnej dobe považované za bezpečné. Preto sa dnes využívajú tunely pomocou protokolu *IP Security* (IPSec) prípadne pre remote access VPN je to protokol OpenVPN pracujúci na aplikačnej vrstve.



Obr. 3.15: Porovnanie site-to-site a remote access VPN

Mapovanie siete a objavovanie zariadení

Protokoly objavujúce zariadenia ako LLDP a *Cisco Discovery Protocol* (CDP) umožňujú získanie mnohých informácií o susedných pripojených zariadeniach, ako napríklad IP adresy, informácie o VLAN, operačnom systéme a mnohé ďalšie. Na tieto protokoly existuje veľké množstvo útokov s veľmi závažnými následkami. Často sa tieto protokoly používajú pri IP telefónii a preto ich nie je možné plošne vypnúť, ideálne by sa mali zakázať aspoň na rozhraniach, kde nepotrebné operovať.

Získavanie smerovacích informácií a masku podsiete je možné aj pomocou správy *Internet Control Message Protocol* (ICMP) typu redirects a mask reply. Problémom je aj directed broadcast, ktorý umožňuje získať ICMP odpoveď na správu ICMP

Echo zaslanú na broadcast adresu smerovača. Zariadenia od spoločnosti Cisco majú túto funkciu už dlhšiu dobu z bezpečnostných dôvodov zakázanú.

Mapovanie siete je možné aj pomocou *Multicast Listener Discovery* (MLD) a *Internet Group Management Protocol* (IGMP) Query správ, prípadne správami ICMP Echo na adresu ff02::1 a 224.0.0.1 [33][32]. Na zabránenie tohto útoku je možné použiť pravidlá v ACL.

Bezpečnostným problémom, ale aj systémom porušujúci fakt, že smerovač oddeľuje siete a broadcast doménu je proxy ARP. Tento systém umožňuje preposielanie ARP správ smerovačom do ďalších sietí. Využíva sa napríklad aj pri VPN, kedy chceme spojiť dve siete na vrstve sieťového rozhrania.

Nepoužívané a nebezpečné služby

Sieťové zariadenia sa často predávajú s rôznymi spustenými službami a tieto predvolené nastavenia, ktoré nie sú potrebné, môžu byť terčom útokov, a preto by mali byť vypnuté [10]. Keďže administrátor tieto funkcie nepoužíva, tak im ani nevenuje pozornosť pri zabezpečovaní. Typickými príkladmi sú administrácia pomocou protokolu *Hypertext Transfer Protocol* (HTTP) prípadne spustený HTTP server a podobne.

Ostatné

Pre korektné fungovanie viacerých protokol je vhodné využívať ako zdroj Loopback rozhranie. Preto je dobrým zvykom definovať jedno Loopback rozhranie na zariadení, ktoré je dostupné hneď po štarte, nie ako fyzické rozhrania a môže byť užitočné ako identifikátor zariadenia pre viaceré protokoly. Toto rozhranie respektíve IP adresa sa používa ako zdrojová pri protokoloch *Network Time Protocol* (NTP), RADIUS, Tacacs+, SNMP, Syslog, SSH a tiež k identifikácií staníc dynamických smerovacích protokolov [5] [7] [10].

4 Návrh

4.1 Požiadavky na aplikáciu a existujúce riešenia

Kľúčovou vlastnosťou je modularita navrhovanej aplikácie, vďaka ktorej bude možné pridávať a definovať nové moduly na odhaľovanie a opravu nedostatkov alebo meniť existujúce pri zmene syntaxe a sémantike príkazov. Modularita taktiež umožňuje vytvorenie a podporu ďalších výrobcov a operačných systémov sieťových zariadení. Existujúce riešenia sú zväčša zamerané iba na jedného výrobcu a operačný systém, pričom program je jeden zdrojový súbor, ktorý bez dobrej znalosti kódu je problematické upraviť a rozšíriť. Preto jednotlivé overovania odporúčaní a ich následná oprava bude každé v separátnom module, ktorý budú musieť dodržať určité vstupy a výstupy, teda akési *Application programming interface* (API). Existujúce riešenia nedisponujú žiadnym generovaním opravnej konfigurácie na základe nálezu nedostatku, preto vzniknutá aplikácia bude podporovať aj vygenerovanie nápravy.

Príkladom open-source riešenia je *Cisco Config Analysis Tool* [50], ktorý čerpá odporúčania z jednej z kníh [7], pomocou ktorej boli vytvorené aj odporúčania v tejto práci. V tomto riešení však chýba veľa dôležitých prevádzkových a bezpečnostných odporúčaní z dôvodu, že námetom na kontrolný zoznam pri zostavovaní aplikácie bola iba jedna kniha. Taktiež podporuje iba jedného výrobcu sieťových zariadení a chýba mu modularita, nerozlišuje odporúčania a kontrolu ich prítomnosti na základe umiestnenia sieťového zariadenia v hierarchickom modeli. Existujúci nástroj *Cisco Config Analysis Tool* obsahuje kontrolu iba na niektoré bezpečnostné nastavenie pre protokol IPv6. Nástrojom s podobnými vlastnosťami a nedostatkami je aj *Router Auditing Tool* [51], ktorý má navyše aj *graphical user interface* – *grafické užívateľské rozhranie* (GUI). Existuje niekoľko rozšírení aj pre nástroj *Nessus*, ktoré overujú dodržiavanie odporúčaní a podľa zistení čerpajú z CIS Benchmark [10] prípadne z ekvivalentu benchmarku pre zariadenia od výrobcu Juniper. Taktiež však nepodporujú zjednanie nápravy a ignorujú umiestnenie zariadenia v topológii.

Výhodou výsledného programu je aj, že kontrolný zoznam vznikol z viacerých knižných odporúčaní a benchmarkov organizácií zaoberajúcimi sa danou problematikou. Program bude umožňovať spúšťanie modulov zodpovedných za nájdenie a odstránenie nedostatkov na základe definovaného umiestnenia zariadenia v hierarchickom modeli siete. Tým sa zamedzí generovaniu falošne pozitívnych správ, ktoré by vznikli v dôsledku overovania nerelevantných požiadavkov na zariadenie v danej vrstve modelu. V neposlednom rade bude riešenie zdarma s možnosťou nahliadnuť a modifikovať respektíve rozšíriť kód. Program bude umožňovať kontrolu odporúčaní aj pre protokol IPv6, ktorým sa príliš nezaobrá väčšina odporúčaní a benchmarkov.

Kľúčové vlastnosti:

- Modularita – každé overenie a náprava bude v zvlášť súbore prihliadajúc na výrobcu a operačný systém pre ktoré je určené.
- Prispôsobenie na ďalších výrobcov – definovanie API pre moduly na budúcu podporu pre zariadenia od viacerých výrobcov a ich operačných systémov.
- Zjednanie nápravy – pri nájdení nedostatku vygenerovanie opravného nastavenia.
- Podpora IPv6 – detekcia zlého alebo chýbajúceho nastavenia a následná náprava pre protokol IPv6.
- Hierarchický model – skenovanie nedostatkov typických pre jednotlivé vrstvy, v ktorých sa zariadenia nachádzajú a tým zníženie falošne pozitívnych varovaní.
- Definuje závažnosti – každý nájdený nedostatok je hodnotený na 4 stupňovej škále.
- Personalizácia – definovanie modulov, ktoré sa spustia pre jednotlivé vrstvy, zmena závažnosti nájdených nedostatkov v konfiguračných súboroch
- Zoznam útokov a problémov verzie operačného systému
- Vygenerovanie správy s nedostatkami

4.2 Rozdelenie príkazov

Na zariadeniach od firmy Cisco s operačným systémom IOS bol vykonaný rozbor možných príkazov a ich foriem zápisu a početnosti výskytu v konfigurácií. Tento rozbor bol spravený z dôvodu, že niektoré príkazy sa môžu opakovať a zároveň jeden druh príkazu môže byť konfigurovaný v rôznych kontextoch a teda neprítomnosť v jednom kontexte automaticky neznamená nedostatok v konfigurácií. Na základe rozboru boli rozdelené príkazy na konfiguráciu sieťových zariadení do nasledujúcich štyroch kategórií:

1. Maximálne s jedným výskytom v konfigurácii – príkladom môže byť verzia protokolu SSH.

Výpis 4.1: Konfigurácia verzie protokolu SSH

```
Router(config)#ssh version 2
```

1

2. Viacnásobný výskyt viazaný na rozhranie – typickým príkladom je zabezpečenie portu s definovaním maximálneho počtu povolených *Media Access Control* (MAC) adries.

Výpis 4.2: Konfigurácia maximálneho počtu povolených MAC adries na porte

```
Router(config)#interface FastEthernet0/1
```

1

```
Router(config-if)#switchport port-security mac address  
maximum 1
```

2

3. Viacnásobný výskyt v konfigurácii – tieto príkazy konfigurujú rôzne služby, napríklad autentizáciu správ OSPF.

Výpis 4.3: Konfigurácia autentizácie OSPF na porte alebo v procese

```
Router(config)#interface FastEthernet0/1
```

1

```
Router(config-if)#ip ospf message-digest-key 1 md5 heslo
```

2

```
Router(config-if)#ip ospf authentication message-digest
```

3

```
Router(config)#router ospf 1
```

4

```
Router(config)#area 0 authentication message-digest
```

5

```
Router(config)#area 0 authentication key-chain 1
```

6

4. Všeobecný príkaz pre celé zariadenie a zároveň viacnásobný výskyt viazaný na rozhranie – s týmto nastavením je možné sa stretnúť pri protokole *Link Layer*

Discovery Protocol (LLDP), ktorý je možné zapnúť pre všetky porty globálne a následne selektovať porty, na ktorých nebude bežať.

Výpis 4.4: Konfigurácia protokolu LLDP a vypnutie protokolu pre jeden port

Router(config)#lldp run	1
Router(config)#interface FastEthernet0/1	2
Router(config-if)#no lldp receive	3
Router(config-if)#no lldp transmit	4

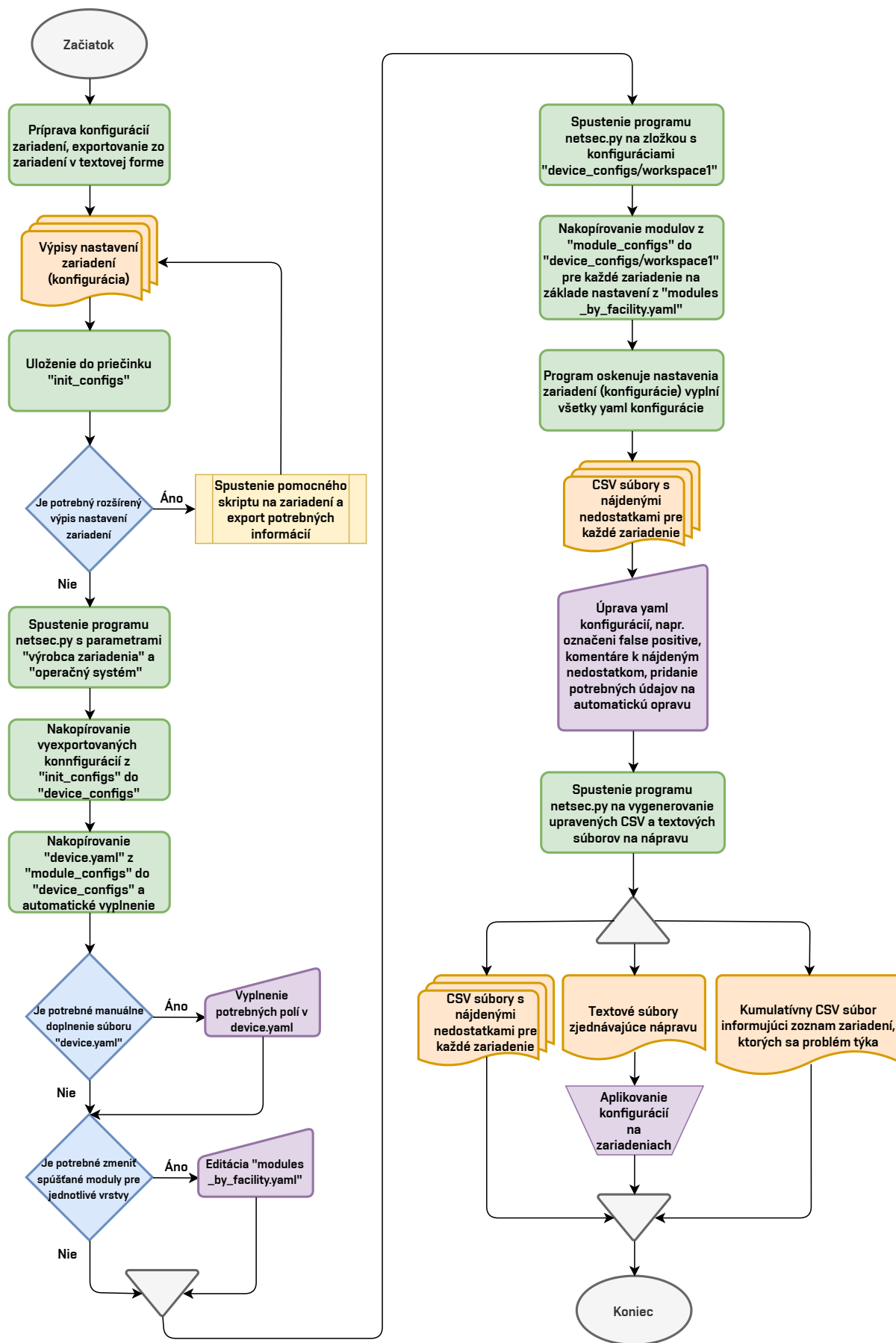
4.3 Rozdelenie sieťových prvkov

Sieť je dnes navrhovaná zväčša podľa hierarchického modelu opísaného v kapitole 3.1. Preto sa aj problémy a útoky v návrhu zatriedujú podľa vrstvy, ktorú ovplyvňujú. V praxi sa však v menších sieťach funkcie jednotlivých vrstiev zlučujú, a preto boli okrem štandardných vrstiev nad rámec hierarchického modelu definované nasledujúce:

- CORE/EDGE – core vrstva, prípadne s funkciou hraničného prvku.
- DIST – distribučná vrstva.
- ACC – prístupová vrstva.
- COLALL – všetky vyššie zmienené vrstvy zlúčené do jednej.
- COLDISTACC – zlúčená distribučná a prístupová vrstva.
- COLCOREDIST – zlúčená core a distribučná vrstva.

4.4 Princíp fungovania

Vstup programu počíta s predpripravenými konfiguráciami v textovej podobe, tie sú často dostupné z pravidelných záloh. Môže sa stať, že nie všetky nastavenia potrebné na dôsledné oskenovanie sú k dispozícii a preto je možné vyexportovať potrebné výstupy zo zariadenia pomocou skriptu, ktorý by bol spustiteľný na zariadení. Program umožní automaticky vyplniť polia v konfiguračnom súbore pre zariadenie `device.yaml`, no v prípade nedostačujúcich informácií zo stiahnutých konfigurácií je potreba manuálne vyplniť niektoré parametre, napríklad vrstvu, na ktorej zariadenie pracuje. Po úspešnom oskenovaní bude možné označiť nálezy ako falošne pozitívne a okomentovať tento dôvod, následne po takomto označení nebude generovaná náprava na nález na danom zariadení. Výstupom bude správa v CSV formáte s nedostatkami, informáciou o zjednanej náprave alebo označení falošne pozitívneho nálezu. Aplikovanie nápravy bude zjednané manuálne nakopírovaním tejto nápravy na zariadenie prípadne pomocou programov na hromadné nasadenie ako napríklad Ansible.



Obr. 4.1: Vývojový diagram opisujúci prácu s programom a tok dát v programe

Hierarchická štruktúra

Nasledujúca štruktúra súborov s komentármi vyobrazuje hierarchiu uloženia potrebných súborov na vykonávanie skenovania nedostatkov a zjednanie náprav. Súbor `hostname1_fix_hash` obsahuje namiesto slova “hash” skutočný hash súboru `hostname1_config.txt`, aby bolo zrejmé, ku ktorej verzii konfigurácie zariadenia patrí a v prípade aktualizovania a pridania novej konfigurácie do `init_configs` nedošlo k nejednoznačnosti. Nové konfigurácie stiahnuté zo zariadenia sa schválne nedávajú do zložky `device_configs`, keďže táto zložka môže obsahovať už nejakú nápravu a správu k predchádzajúcej konfigurácii, a preto by mohol vzniknúť konflikt a nebolo by jasné ku ktorej verzii konfigurácie výstupy programu patria. Program bude uchovávať taktiež históriu jednotlivých skenovaní a náprav, pričom pri iniciovaní nového skenovania a prítomnosti novej verzie konfigurácie zariadenia, príde k premiestneniu aktuálnych výstupov do podzložky s hashom prisluchajúcim konfigurácií `hostname1_old_hash`.


```

/ .....koreňový adresár programu
├── netsec.py ..... hlavný program
├── modules .....adresár so šablónami konfiguračných súborov
│   ├── cisco ..... výrobca sieťového zariadenia
│   │   ├── ios ..... operačný systém bežiaci na zariadení
│   │   │   ├── device.yaml .....šablóna na uloženie základných informácií o zariadení
│   │   │   ├── aaa
│   │   │   │   ├── aaa.py ..... modul zodpovedný za skenovanie a nápravu
│   │   │   │   └── aaa.yaml ..... šablóna konfiguračného súboru k modulu
│   │   │   ├── cdp
│   │   │   │   ├── cdp.py
│   │   │   │   └── cdp.yaml
│   │   └── modules_by_facility.yaml .... súbor s definíciou, ktoré moduly budú
│   │       spustené pre zariadenia na konkrétnej vrstve modelu
│   ├── hp
│   ├── juniper
│   │   └── junos
├── device_configs ... adresár s výstupmi, konfiguráciami a súbormi na ich nápravu
│   ├── workspace1 ..... adresár jednej topológie/siete
│   │   ├── summary_report ..... správa s mapovaním nedostatkov-zariadenie
│   │   ├── hostname1
│   │   │   ├── device.yaml ..... základné informácie o konkrétnom zariadení
│   │   │   ├── aaa.yaml ..... konfiguračný súbor k modulu s nájdenými nedostatkami
│   │   │   ├── cdp.yaml
│   │   │   ├── report_hostname1.csv ... detailnejšia správa pre konkrétne zariadenie
│   │   │   ├── version ..... informácie o verzii operačného systému a jeho chýb
│   │   │   ├── hostname1_config.txt ..... aktuálne skenovaná konfigurácia
│   │   │   ├── hostname1_fix_hash ..... súbor s nápravnou konfiguráciou
│   │   │   └── hostname1_old_hash .. predchádzajúce konfigurácie, zistenie a nápravy
│   │   └── hostname2
│   └── workspace2
├── init_configs .....adresár s novými skopírovanými konfiguráciami zariadení
│   ├── workspace1
│   │   ├── version
│   │   ├── hostname1_config.txt
│   │   └── hostname2_config.txt
│   └── workspace2
└── current_output .....aktuálne správy a nápravy na jednom mieste
    ├── workspace1_hostname1_fixhash
    └── workspace1_report_hostname1.csv

```

4.5 Zoznam odporúčaní

V súčasnej dobe existuje mnoho odporúčaní, štandardov a benchmarkov, ktoré sa zaoberajú bezpečnosťou a správnou konfiguráciou sieťových zariadení. V mnohých prípadoch sú buď príliš všeobecné a teda sieťoví inžinieri majú problém zistiť, čo daným odporúčaním autor myslel a ako ho implementovať, alebo sú určené iba pre zariadenia od jedného výrobcu. Problémom je taktiež, že väčšina odporúčaní, štandardov a benchmarkov sa nie úplne prekrývajú, a teda je potrebné pri nastavovaní a audite zariadení čerpať s mnohých naraz. Nižšie uvedené výsledné tabuľky obsahujú odporúčania z odbornej literatúry, štandardov a benchmarkov verejne dostupných a používaných v produkčnom nasadení. Výhodou je aj fakt, že obsahujú odporúčania vychádzajúce z problémov IPv6, ktoré nie sú často v štandardoch a benchmarkoch dostupné. Podrobná tabuľka s mapovaním odporúčaní na príkazy pre zariadenia Cisco s operačným systémom IOS je v prílohe TODO príloha

Zariadenia Cisco boli pre túto prácu vybrané z dôvodu, že spoločnosť Cisco je lídrom ktorý udáva trend, ich zariadenia sú celosvetovo v korporáciách veľmi rozšírené a mnoho literatúry a benchmarkov sa odvoláva na nastavenia týchto prístrojov s udávanými príkladmi konfigurácie. Taktiež sú tieto zariadenia dobrým referenčným príkladom pre hľadanie alternatívy v zariadeniach od iných výrobcov.

Tabuľky sú rozdelené do skupín podľa protokolu prípadne okruhu problému, ktorému sa venujú. V tabuľkách je možné vidieť, že odporúčania sú zatriedené podľa viacerých kritérií. V prvom rade sú to roviny (plane), ktoré nie sú dôležité pre následnú automatickú konfiguráciu a odhaľovanie problémov, ale na vytvorenie si obrazu, ktorá časť rovin je kritická a postihnuteľná najviac.

Stĺpec závažnosť (severity) vznikol na základe predpokladaných závažností. Tento atribút bude možné zmeniť v konfiguračnom súbore každého modulu v závislosti na riziku, ktoré sa pre danú topológiu a firmu vyhodnotí za pomoci manažmentu rizík opísaného v kapitole 2. Tento atribút sa nenachádza v žiadnom štandarde ani benchmarku, z ktorého vytvorený zoznam odporúčaní čerpal, no je veľmi dôležitý z hľadiska, že nie všetky nedostatky sú rovnako závažné a nemajú rovnaký dopad. Hodnoty, ktoré nadobúda sú prebrané zo štandardu CVSS, pričom posledný interval **none** reprezentujúci nulové riziko respektíve závažnosť je zamenený za kľúčové slovo **notify**. K tejto zmene prišlo z dôvodu, že problémy s nulovým rizikom nie sú súčasťou návrhu a nemá zmysel ich riešiť. V prípade, že bude nález falošne pozitívny alebo riziko bude akceptované, tak sa táto skutočnosť uloží do konfiguračného súboru. Závažnosť **notify** bude použitá v prípade prítomnosti monitorovania portu pomocou zrkadlenia portu alebo NetFlow/sFlow. Jedná sa totiž o technológie potrebné na monitorovanie prevádzky z legislatívnych alebo bezpečnostných dôvodov. Riziko existuje iba pri nesprávnom nastavení zdrojov monitorovania a cieľu pre zber

dát, a preto je dobré vedieť pri audite o prítomnosti tohto nastavenia.

Posledným rozdelením je vrstva, na ktorej zariadenie pracuje (facility layer), nakoľko rozdelenie podľa zariadení nie je dostatočné, pretože napríklad L3 prepínač môže byť použitý na ktorejkoľvek vrstve hierarchického modelu a každá vrstva má určité špecifiká, ktoré neobsahuje iná vrstva. Každý konfiguračný súbor popisujúci zariadenie bude obsahovať informáciu, do ktorej vrstvy patrí a na základe toho bude môcť program rozhodnúť, ktoré moduly zodpovedné za nájdenie problému a jeho vyriešenie budú nad konfiguračným súborom zariadenia spustené. Taktiež bude možné meniť, dopĺňať a zakázať spúšťanie modulov pre jednotlivé zariadenia, pokiaľ by v danej topológii nevyhovovalo rozdelenie z tabuliek uvedených nižšie.

Vrstva, na ktorej zariadenie operuje, ako aj definované zariadenie, ktorého sa odporúčanie a opatrenie týka nie sú súčasťou žiadneho kontrolného zoznamu, benchmarku ani štandardu, z ktorého bolo čerpané. Sieťový administrátor by preto musel sám vyvodiť záver, ktoré odporúčania a postupy bude aplikovať na jednotlivé zariadenia a vrstvy hierarchického modelu. Preto vytvorená tabuľka odporúčaní už obsahuje aj zoznam zariadení, ktorých sa opatrenie týka.

Z dôvodu šetrenia priestoru boli hodnoty nadobúdajúce stĺpce Plane a Severity skrátené na iniciály slov reprezentujúce tieto hodnoty. Ich celé názvy je možné nájsť v kapitole 4.3 respektíve 2.1. Stĺpec Facility layer navyše obsahuje hodnotu **A**, ktorej význam znamená, že toto odporúčanie sa vzťahuje na všetky zariadenia bez ohľadu, na akej vrstve operujú.

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
1	Nepovolený prístup k manažovaniu zariadenia	Vytvoriť a aplikovať ACL pre OOB, Telnet, SSH a pod. a zaznamenať v logu prístupy	M	C	A	Hardening Cisco Routers [44] CIS Cisco IOS 15 Benchmark [10]
2	Neautorizovaný prístup cez nepoužívané a nebezpečné protokoly na manažment zariadení	Vypnúť nepoužívané protokoly na prístup k manažovaniu zariadení (telnet a pod.)	M	H	A	CIS Cisco IOS 15 Benchmark [10] Cisco Guide to Harden Cisco IOS Devices [7]
3	Nepovolený prístup k manažmentu konfigurácie zariadenia	Vypnutie odchádzajúcich spojení pre protokoly na manažment zariadení pokiaľ sa nepoužívajú (telnet a pod.)	M	H	A	Cisco Guide to Harden Cisco IOS Devices [7]
4	Prístup bez požadovaných prístupových údajov	Nakonfigurovanie protokolov na manažment zariadení, aby požadovali prístupové údaje (telnet a pod.)	M	C	A	CIS Cisco IOS 15 Benchmark [10]
5	Nekonzistenia konfiguračných súborov pri zmenách konfigurácie viac ako jedným administrátorom	Povolit súčasne iba jednému administrátorovi vykonávanie zmien v konfigurácii	M	H	A	Cisco Guide to Harden Cisco IOS Devices [7]
6	Nepoužívanie zabezpečeného protokolu na manažment zariadení môže viesť k odposluchu	Zapnutie SSH	M	C	A	CIS Cisco IOS 15 Benchmark [10] Cisco Router Hardening [19]
7	Nebezpečná verzia 1 protokolu SSH	SSH verzia 2	M	C	A	Cisco CCNA Security Study Guide [3]

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
8	Útok na krátky RSA kľúč	Dĺžka RSA kľúča minimálne 2048 bitov	M	C	A	CIS Cisco IOS 15 Benchmark [10] Transitioning the Use of Cryptographic Algorithms and Key Lengths [11]
9	Dlhé neaktívne sedenie môže byť zneužitá alebo aj fyzický prístup útočníka k aktívnemu sedeniu môže viesť k zmene konfigurácie	SSH čas vypršania sedenia	M	M	A	CIS Cisco IOS 15 Benchmark [10] Cisco Router Hardening [19]
10	Hádanie hesla k RSA kľúču	SSH maximálny počet neúspešných pokusov	M	H	A	Cisco router configuration handbook [45] Cisco IOS 23 - Autentizace uživatele na switchi vůči Active Directory [38]
11	Útok hrubou silou na zistenie prihlasovacích údajov	Špecifikovať čas po ktorý nie je možné po N pokusoch sa prihlásiť	M	H	A	Cisco router configuration handbook [45] Cisco IOS 23 - Autentizace uživatele na switchi vůči Active Directory [38]
12	Prihlásenie na zariadenie nie je možné kvôli zablokovaniu pre príliš veľa neúspešných pokusov	Povolenie prístupu administrátorovi na základe IP adresy, keď je protokol na manažovanie zariadení nedostupný kvôli DOS útoku	M	M	A	Cisco router configuration handbook [45] Cisco IOS 23 - Autentizace uživatele na switchi vůči Active Directory [38]

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
13	Dlhé neaktívne sedenie môže byť zneužitá alebo aj fyzický prístup útočníka k aktívne sedeniu môže viesť k zmene konfigurácie	Čas vypršania sedenia pre protokol na manažovanie zariadení	M	M	A	CIS Cisco IOS 15 Benchmark [10] Cisco Router Hardening [19] Cisco SAFE Reference Guide [20]
14	Možné prihlásenie do zariadenia cez telnet keď je prítomné SSH	Zakázať telnet ak je SSH aktívne	M	C	A	CIS Cisco IOS 15 Benchmark [10] Cisco Router Hardening [19]
15	Útočník nie je informovaný o právnych následkoch	Právne upozornenie pri prístupe k zariadeniu	M	L	A	Cisco CCNA Security Study Guide [3] CIS Cisco IOS 15 Benchmark [10] Cisco Router Hardening [19]
16	Nepovolená zmena konfigurácie zariadenia	Vytvorenie hesla na editovanie konfigurácie zariadenia	M	C	A	CIS Cisco IOS 15 Benchmark [10] Cisco Router Hardening [19]
17	Nepovolený prístup k manažmentu konfigurácie zariadenia	Lokálne zabezpečené účty	M	C	A	Cisco Guide to Harden Cisco IOS Devices [7] CIS Cisco IOS 15 Benchmark [10]
18	Centrálna správa prihlásení a dohľadateľnosť zmien v konfigurácií	Definovanie a povolenie AAA serveru na prihlásenie a definovanie záložného prihlásenia	M	H	A	Hardening Cisco Routers [44] CIS Cisco IOS 15 Benchmark [10] Cisco CCNA Security Study Guide [3] Cisco Router Hardening [19]
19	Centrálna správa prihlásení a dohľadateľnosť zmien v konfigurácií	Definovanie a povolenie AAA serveru na editáciu konfigurácií a definovanie záložného prihlásenia	M	M	A	CIS Cisco IOS 15 Benchmark [10] Cisco Router Hardening [19]

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
20	Hádanie prístupových údajov	Definovanie maximálneho počtu neúspešných pokusov o prihlásenie a následné zablokovanie účtu	M	H	A	CIS Cisco IOS 15 Benchmark [10] Cisco Router Hardening [19]
21	Prihlásenie bez prihlasovacích údajov	Zakázať záložné prihlásenie bez poskytnutia autentizačných prostriedkov	M	C	A	Cisco Guide to Harden Cisco IOS Devices [7]
22	AAA používa primárne lokálne účty namiesto centralizovaných na serveri	AAA nesmie používať ako prvú možnosť prihlásenia lokálny účet	M	H	A	CIS Cisco IOS 15 Benchmark [10] Cisco Router Hardening [19]
23	Používateľ prihlásený do zariadenia môže spúšťať akékoľvek príkazy	Nastavenie AAA autorizácie pre spúšťanie príkazov. V prípade výpadku AAA serveru, bude užívateľ odhlásený a následne prihlásený podľa záložného prihlásenia, aby mu nebolo pridelené vysoké oprávnenie umožňujúce vykonávať príkazy, na ktoré nemá právo	M	H	A	Cisco Router Hardening [19] Cisco Guide to Harden Cisco IOS Devices [7]
24	Administrátor vloží zlý príkaz a po čase je ho nemožné dohľadať a zjednať nápravu	Nastavenie AAA účtovania respektíve logovania pripojení a vykonaných príkazov	M	H	A	CIS Cisco IOS 15 Benchmark [10]
25	AAA zdrojové rozhranie nie je rovnaké pri každom reštarte	Definovanie loopback zdrojového rozhrania pre AAA	M	M	A	CIS Cisco IOS 15 Benchmark [10]

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
26	SSH zdrojové rozhranie nie je rovnaké pri každom reštarte	Definovanie loopback zdrojového rozhrania pre SSH	M	M	A	CIS Cisco IOS 15 Benchmark [10]
27	DOS útok na štandardný SSH port 22	Špecifikovanie iného portu pre SSH ako štandardného alebo aplikovanie Port Knocking [46]	M	H	A	Port Knocking [46]

Tab. 4.1: Odporúčania k prístupu na manažment zariadení

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
1	Vloženie a manipulácia so smerovacími informáciami	Autentizácia smerovacích protokolov (nie heslá v otvorenej podobe)	C	H	CORE/EDGE DIST COLCOREDIST COLDISTACC COLALL	Cisco CCNA Security Study Guide [3] Cisco Guide to Harden Cisco IOS Devices [7] CIS Cisco IOS 15 Benchmark [10]
2	OSPF virtuálne linky degradujú výkon	Vypnutie virtuálnych liniek pre OSPF	C	H	CORE/EDGE DIST COLCOREDIST COLDISTACC COLALL	Designing Cisco network service architectures [49]
3	Koncové zariadenie, užívateľ a útočník môžu vidieť smerovacie správy a topológiu siete alebo pripojenie škodlivého zariadenia, ktoré vysielajú a prijímajú smerovacie správy	Špecifikovanie rozhraní, ktoré nebudú prijímať routovacie informácie	C	H	CORE/EDGE DIST COLCOREDIST COLDISTACC COLALL	OSPF Security: Attacks and Defenses [17]

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
4	Nemožnosť sprevádzkovať procesy smerovacích protokolov v určitých prípadoch pri použití IPv6	Špecifikovanie identifikátorov smerovacích protokolov pre každý router (router ID)	C	M	CORE/EDGE DIST COLCOREDIST COLDISTACC COLALL	Protocol-Independent Routing Properties Feature Guide [48] CCNA Routing and Switching Study Guide [8]
5	Vysledovateľnosť nefunkčnosti routovacieho protokolu a nesprávneho nastavenia	Zaznamenanie zmeny v logu pri zmenách v smerovaní	C	M	CORE/EDGE DIST COLCOREDIST COLDISTACC COLALL	Cisco SAFE Reference Guide [20]
6	Škodlivé vloženie smerovacích informácií informácií, vzdialený útok	TTL security	C	H	CORE/EDGE DIST COLCOREDIST COLDISTACC COLALL	OSPF Security: Attacks and Defenses [17] Cisco Guide to Harden Cisco IOS Devices [7]
7	Nesprávne smerovanie kvôli sumarizáciám	Vypnutie automatickej sumarizácie smerovacích protokolov	C	H	CORE/EDGE DIST COLCOREDIST COLDISTACC COLALL	CCNA Routing and Switching Study Guide [8]
8	DOS útok na stanicu, cez ktorú bola špecifikovaná cesta a teda nemožnosť komunikácie s koncovým bodom. Alebo zosnovanie MITM útoku	Vypnutie IP source routing	C	C	CORE/EDGE DIST COLCOREDIST COLDISTACC COLALL	CIS Cisco IOS 15 Benchmark [10]
9	DOS útok pomocou podvrhutej IP adresy alebo vzdialený útok na smerovací protokol	Zapnutie reverse path forwarding strict/loose mode	C	H	CORE/EDGE DIST COLCOREDIST COLDISTACC COLALL	OSPF Security: Attacks and Defenses [17] Network Security Auditing [5] CIS Cisco IOS 15 Benchmark [10]

Tab. 4.2: Odporúčania pre smerovanie

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
1	IP spoofing	Špecifikácia ACL na zakázanie a logovanie privátnych a špeciálnych IP adries z RFC 1918, RFC 3330	C	C	CORE/EDGE COLCOREDIST COLALL	Network Security Auditing [5] Cisco Guide to Harden Cisco IOS Devices [7] CIS Cisco IOS 15 Benchmark [10]
2	IP spoofing	Špecifikácia ACL na zakázanie a logovanie špeciálnych IPv6 adries z RFC 5156	C	C	CORE/EDGE COLCOREDIST COLALL	Network Security Auditing [5] Cisco Guide to Harden Cisco IOS Devices [7] CIS Cisco IOS 15 Benchmark [10]
3	IPv6 Next Header, IPv6 Fragmentation útok	ACL blokujúce nerozpoznané rozšírené hlavičky	C	C	A	Bezpečné IPv6: trable s hlavičkami [16] Bezpečné IPv6: vícehlavý útočník [15]
4	DOS útok alebo pokus o prístup k tomu, čo nie je povolené	Logovanie pravidiel zahodenia paketov v ACL	M	M	A	Hardening Cisco Routers [44]
5	Packety budú spracovávané v CPU, ktoré môže byť preťažené a môže byť zmenené smerovanie na obídenie bezpečnostnej kontroly	Zahadzovanie IPv4 paketov s rozšírenou hlavičkou (IP Options filtering)	C	C	CORE/EDGE DIST COLCOREDIST COLDISTACC COLALL	Cisco Guide to Harden Cisco IOS Devices [7]
6	Komplexné bezpečnostné hrozby a narušenie bezpečnosti	Nastavenie IDS/IPS ak to zariadenie podporuje	C	H	CORE/EDGE COLCOREDIST COLALL	Cisco router configuration handbook [45]

Tab. 4.3: Odporúčania pre filtrovanie prevádzky

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
1	Nízky stav voľnej pamäte	Nastavenie notifikácie pri dochádzaní pamäte	M	M	A	Cisco Guide to Harden Cisco IOS Devices [7] Cisco SAFE Reference Guide [20]
2	Logovacie správy nemôžu byť zaznamenané kvôli nedostatku pamäte	Rezervovanie pamäte pre kritické notifikácie pri nedostatku pamäte	M	H	A	Cisco Guide to Harden Cisco IOS Devices [7] Cisco SAFE Reference Guide [20]
3	Vysoké zataženie CPU	Nastavenie notifikácie vysokom zatažení CPU	M	M	A	Cisco Guide to Harden Cisco IOS Devices [7] Cisco SAFE Reference Guide [20]
4	Vysoké zataženie zariadenia spôsobilo nemožnosť prihlásenia k nemu	Rezervovanie pamäte preprotokoly na manažment zariadení pri nedostatku pamäte	M	H	A	Cisco Guide to Harden Cisco IOS Devices [7]

Tab. 4.4: Odporúčania pri vysokom zatažení

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
1	Skenovanie a zistenie informácií o sieti za pomoci protokolu CDP a využitie bezpečnostných chýb	Zakázanie protokolu CDP	M	C	A	CIS Cisco IOS 15 Benchmark [10] Cisco Router Hardening [19]
2	Skenovanie a zistenie informácií o sieti za pomoci protokolu LLDP a využitie bezpečnostných chýb	Zakázanie protokolu LLDP	M	C	A	Cisco CCNA Security Study Guide [3]

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
3	Proxy ARP môže viesť k obídeniu PVLAN a rozširuje broadcast doménu	Vypnutie Proxy ARP	C	C	CORE/EDGE DIST COLCOREDIST COLDISTACC COLALL	CIS Cisco IOS 15 Benchmark [10] Cisco Router Hardening [19]
4	Útočník môže zistiť, že IP adresa, na ktorú skúšal ping je nesprávna	Vypnutie spáv ICMP Unreachable	D	H	CORE/EDGE DIST COLCOREDIST COLDISTACC COLALL	Cisco Guide to Harden Cisco IOS Devices [7]
5	Útočník môže zistiť masku podsiete pomocou ICMP Mask reply	Vypnutie spáv ICMP Mask reply	D	H	CORE/EDGE DIST COLCOREDIST COLDISTACC COLALL	Hardening Cisco Routers [44]
6	Umožňuje DOS Smurf útok, mapovanie siete pomocou ping na broadcast adresu vzdialenej siete	Vypnutie ICMP echo správ na broadcast adresu, vypnutie directed broadcasts	D	C	CORE/EDGE DIST COLCOREDIST COLDISTACC COLALL	Cisco Router Hardening [19] Hardening Cisco Routers [44]
7	Útočník môže zistiť smerovacie informácie alebo vyťažiť CPU	Vypnutie spáv ICMP Redirects	D	H	CORE/EDGE DIST COLCOREDIST COLDISTACC COLALL	Cisco Guide to Harden Cisco IOS Devices [7]
8	Mapovanie sete pomocou pingu na multicast adresu všetkých uzlov a MLD/IGMP Query Overload a Smurf útok	ACL blokujúce ICMP echo request na multicast adresu všetkých uzlov a MLD/IGMP Query na prístupových portoch	C	M	DIST COLDISTACC ACC	Bezpečné IPv6: trable s multicastem [32] MLD Considered Harmful [33]

Tab. 4.5: Odporúčania na zamedzenie mapovanie siete

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
1	Nemožná identifikácia zariadenia	Vytvoriť hostname	M	L	A	CIS Cisco IOS 15 Benchmark [10]
2	Nemožnosť vzdialeného prístupu	Vytvoriť doménové meno	M	L	A	CIS Cisco IOS 15 Benchmark [10]
3	Identifikácia pravidiel v ACL	Popis každého pravidla v ACL pre lepšiu identifikáciu	M	L	A	Cisco Guide to Harden Cisco IOS Devices [7]
4	Identifikácia rozhrania	Popis každého rozhrania	M	L	A	CCNA Routing and Switching Study Guide [8]
5	Nemožnosť identifikácie účelu VLAN	Pridanie mena k VLAN	C	L	DIST COLDISTACC ACC COLALL	CCNA Routing and Switching Study Guide [8]

Tab. 4.6: Odporúčania na identifikáciu zariadení a nastavení

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
1	Nekonzistencia časov v logoch a problém pričlenenia logov k relevantným incidentom	Nastavenie NTP serveru pre aktuálny čas v logoch	M	H	A	Network Security Auditing [5] Cisco Guide to Harden Cisco IOS Devices [7] CIS Cisco IOS 15 Benchmark [10]
2	Pripojenie servera s rovnakou IP adresou, ale falošným časom	Nastavenie NTP autentizácie	M	H	A	Network Security Auditing [5] Cisco Guide to Harden Cisco IOS Devices [7] CIS Cisco IOS 15 Benchmark [10]
3	NTP zdrojové rozhranie nie je rovnaké pri každom reštarte	Definovanie loopback zdrojového rozhrania pre NTP	M	M	A	Network Security Auditing [5] Cisco Guide to Harden Cisco IOS Devices [7] CIS Cisco IOS 15 Benchmark [10]

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
4	Väčšia bezpečnosť (pub/priv key) NTP a podpora IPv6	Použitie NTP verzie 4	M	M	A	The NTP FAQ and HOWTO [22]
5	Falošný čas od podvrhnutého NTP zdroja	Nastavenie NTP peer s inými sieťovými zariadeniami na krížovú validáciu času a záložný zdroj času	M	M	A	Hardening Cisco Routers [44]

Tab. 4.7: Odporúčania k protokolu NTP

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
1	Odpočúvanie SNMP verzie 1 a 2c	Použitie SNMP verie 3 pokiaľ je SNMP používané	M	C	A	CIS Cisco IOS 15 Benchmark [10] Cisco Router Hardening [19]
2	Modifikovanie konfigurácie pomocou SNMP	Obmedzenie SNMP iba na čítanie	M	C	A	CIS Cisco IOS 15 Benchmark [10] Cisco Router Hardening [19] Hardening Cisco Routers [44]
3	Neoprávnený prístup k SNMP informáciám	Obmedzenie SNMP iba pre vybrané IP adresy	M	H	A	CIS Cisco IOS 15 Benchmark [10] Cisco Router Hardening [19]
4	Administrátor nemá povedomie o problémoch na zariadení	Povolenie asynchrónnych správ SNMP TRAP	M	M	A	CIS Cisco IOS 15 Benchmark [10] Cisco Router Hardening [19] Hardening Cisco Routers [44]

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
5	Odpočúvanie SNMP sedenie z dôvodu slabého šifrovania a hashovacej funkcie	Vytvorenie SNMP verzie 3 užívateľa s minimálnym šifrovaním AES 128 bit a hashovacou funkciou SHA	M	C	A	Transitioning the Use of Cryptographic Algorithms and Key Lengths [11] CIS Cisco IOS 15 Benchmark [10] Hardening Cisco Routers [44]
6	Hard identification of SNMP messages from many IPs/ Sťažená identifikácia SNMP správ z rôznych IP	Definovanie lokácie SNMP serveru	M	L	A	Cisco IOS Cookbook [47]
7	SNMP zdrojové rozhranie nie je rovnaké pri každom reštarte	Definovanie loopback zdrojového rozhrania pre SNMP	M	M	A	CIS Cisco IOS 15 Benchmark [10]
8	Zmeny názvov rozhraní medzi reštartami a nemožnosť monitorovania pomocou SNMP	SNMP statické nemenné meno rozhrania aj po reštarte zariadenia	M	H	A	Cisco IOS Cookbook [47]

Tab. 4.8: Odporúčanie pre protokol SNMP

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
1	Administrátor nemá povedomie o problémoch na zariadení	Povolenie logovania protokolom SYSLOG a špecifikovanie IP adresy SYSLOG serveru	M	H	A	CIS Cisco IOS 15 Benchmark [10] Cisco Router Hardening [19]
2	Neprijímanie všetkých dôležitých incidentov na zariadení z protokolu SYSLOG	Špecifikovanie dôležitosti oznámení SYSLOG na INFORMATIONAL	M	M	A	CIS Cisco IOS 15 Benchmark [10]

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
3	SYSLOG zdrojové rozhranie nie je rovnaké pri každom reštarte	Definovanie loopback zdrojového rozhrania pre SYSLOG	M	M	A	Cisco Guide to Harden Cisco IOS Devices [7] CIS Cisco IOS 15 Benchmark [10]
4	Insufficient and non-standard time format in logging messages/ Nedostatočné a neštandardné formáty času pri logovacích správach	Definovanie formátu času pre logovacie a ladiace výstupy	M	M	A	CIS Cisco IOS 15 Benchmark [10] Cisco Router Hardening [19]
5	Administrátor nevidí dôležité incidenty pri prihlásení a konfigurovaní cez konzolu	Vypisovanie SYSLOG správ CRITICAL a dôležitejších do terminálu	M	M	A	Cisco Guide to Harden Cisco IOS Devices [7] CIS Cisco IOS 15 Benchmark [10]
6	Malá vyrovnávacia pamäť pre SYSLOG je dôvodom zahadzovanie správ	Definovanie veľkosti SYSLOG buffera dôležitosti oznámení na INFORMATIONAL	M	H	A	Cisco Guide to Harden Cisco IOS Devices [7]
7	Nepriístupný SYSLOG server spôsobuje zahadzovanie dôležitých syslog správ	Definovanie dočasného úložiska SYSLOG správ v prípade nedostupnosti servera	M	H	A	Cisco Guide to Harden Cisco IOS Devices [7]
8	Problém identifikácie SYSLOG správ s rovnakou časovou značkou	Pridanie sekvenčného čísla ku každej syslog správe	M	L	A	Hardening Cisco Routers [44]

Tab. 4.9: Odporúčania pre protokol Syslog

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
1	MAC Spoofing, MAC Flooding	Definovanie maximálne 1 MAC adresy na port, priradenie MAC adresy na port	C	C	DIST COLDISTACC ACC	CCNA Routing and Switching Study Guide [8]
2	MAC Spoofing, MAC Flooding	Nastavenie režimu narušenia, ktorý vypne port alebo informuje správcu o pripojení nepovoleného zariadenia	C	H	DIST COLDISTACC ACC	CCNA Routing and Switching Study Guide [8]
3	Využívanie siete nepovolenými používateľmi	Zapnutie 802.1x	C	H	DIST COLDISTACC ACC	Lan Switch Security [2] Cisco IOS 11 - IEEE 802.1x, autentizace k portu, MS IAS [35] Cisco IOS 12 - IEEE 802.1x a pokročilejší funkce [36]
4	Útok hrubou silou hádaním prístupových údajov pre 802.1x	Limitovanie maximálneho počtu neúspešných pokusov o autentizáciu 802.1x	C	H	DIST COLDISTACC ACC	Lan Switch Security [2] Cisco IOS 11 - IEEE 802.1x, autentizace k portu, MS IAS [35] Cisco IOS 12 - IEEE 802.1x a pokročilejší funkce [36]
5	DHCP spoofing	DHCP snooping, IPv6 Snooping, DHCPv6 Guard	C	C	DIST COLDISTACC ACC	Lan Switch Security [2] Cisco Guide to Harden Cisco IOS Devices [7] IPv6 First-Hop Security Configuration Guide [34]
6	Příliš veľa DHCP paketov, zaplavenie DHCP paketmi	Odmedziť počet DHCP paketov na nedôverihodných rozhraniach	C	M	DIST COLDISTACC ACC	Lan Switch Security [2] Cisco Guide to Harden Cisco IOS Devices [7] IPv6 First-Hop Security Configuration Guide [34]

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
7	ARP Spoofing	Dynamic ARP Inspection	C	C	DIST COLDISTACC ACC	Cisco CCNA Security Study Guide [3]
8	IP spoofing	IPv4/IPv6 Source Guard	C	C	DIST COLDISTACC ACC	Cisco Guide to Harden Cisco IOS Devices [7] IPv6 First-Hop Security Configuration Guide [34]
9	IPv6 ND Spoofing	IPv6 ND Inspection	C	C	DIST COLDISTACC ACC	Bezpečné IPv6: zkročení zlých směrovačů [28] Bezpečné IPv6 : směrovač se hlásí [27] IPv6 First-Hop Security Configuration Guide [34]
10	Rogue RA, RA Flood, RouterLifeTime=0	RA Guard	C	C	DIST COLDISTACC ACC	Bezpečné IPv6: zkročení zlých směrovačů [28] Bezpečné IPv6 : směrovač se hlásí [27] IPv6 First-Hop Security Configuration Guide [34]
11	Mobilné zariadenia pripojené bezdôtovo spotrebovávajú veľa energie kvôli častým RA správam	RA Throttling	C	L	DIST COLDISTACC ACC	Bezpečné IPv6: trable s multicastem [32] ND on wireless links and/or with sleeping nodes [39]
12	Výčerpanie cache susedov	Statický záznam pre kritické zariadenia (servery) spájajúce IP a MAC adresu a VLAN	C	C	DIST COLDISTACC ACC	Bezpečné IPv6: když dojde keš [30] Bezpečné IPv6: když dojde keš – obrana [31]

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
13	Vyčerpanie cache susedov	Na zabránenie vzdialeného útoku na cache susedov cez internet je potreba nastaviť ACL, kde povolujeme iba komunikáciu s cieľovými IPv6 adresami, ktoré sa nachádzajú v našej sieti	C	C	CORE/EDGE COLCOREDIST COLALL	Bezpečné IPv6: keď dojde keš [30] Bezpečné IPv6: keď dojde keš – obrana [31]
14	Vyčerpanie cache susedov	IP destination Guard (First Hop Security)	C	C	DIST COLDISTACC ACC	Bezpečné IPv6: keď dojde keš [30] Bezpečné IPv6: keď dojde keš – obrana [31]
15	Vyčerpanie cache susedov	Limitovanie času IPv6 adresy v cache susedov	C	C	DIST COLDISTACC ACC	Bezpečné IPv6: keď dojde keš [30] Bezpečné IPv6: keď dojde keš – obrana [31]

Tab. 4.10: First Hop Security útoky a odporúčania

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
1	Rogue root bridge protection (root guard)	Rogue root bridge	C	C	DIST COLDISTACC ACC	Lan Switch Security [2]
2	BPDU protection (BPDU guard)	Pripojenie pripínaču na koncový prístupový port	C	C	DIST COLDISTACC ACC	Lan Switch Security [2]
3	Prístupové porty by sa nemali podieľať na STP procese	Rýchlosť konvergenencie	C	H	DIST COLDISTACC ACC	Lan Switch Security [2]
4	Špeciálne konfigurácie zaisťujúce bezslučkovú topológiu pomocou STP keď nastane jednosmerná komunikácia (Loop Guard)	Jednosmerná komunikácia medzi prepínačmi môže viesť k topológii so slučkami	C	C	DIST COLDISTACC ACC	Designing Cisco network service architectures [49]

Tab. 4.11: Odporúčania pre Spanning Tree Protokol

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
1	Špeciálna VLAN pre manažment na obmedzenie prístupu iba pre administrátorov	Vytvorenie separátnej VLAN pre manažment	C	M	DIST, COLDISTACC, ACC	CCNA Routing and Switching Study Guide [8]
2	Útočníkovi s fyzickým prístupom k portu môže byť pridelený prístup do časti siete, ktorá zodpovedá príslušnej VLAN	Vytvorenie špeciálnej black hole VLAN pre nevyužívané porty	C	C	DIST, COLDISTACC, ACC	Cisco SAFE Reference Guide [20]
3	Predvolenej VLAN je povolené prepnúť na akýkoľvek port, VLAN hopping, double tagging	Odobráť všetky porty z predvolenej VLAN	C	C	DIST, COLDISTACC, ACC	Cisco SAFE Reference Guide [20]

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
4	Predvolenej VLAN je povolené byť prepnutá na akýkoľvek port, VLAN hopping, double tagging	Vytvorenie natívnej VLAN rozdielnej ako predvolená, priradení k trunk portu a povolenie iba potrebných portov	C	C	DIST, COLDISTACC, ACC	Cisco SAFE Reference Guide [20]
5	DTP útok, Switch spoofing útok	Vypnutie dynamického trunkovacieho protokolu a explicitne určiť porty ako prístupové a trunk	C	C	DIST, COLDISTACC, ACC	Cisco SAFE Reference Guide [20]
6	Nový prepínač s vyšším číslom revízie, ale s nesprávnou VLAN databázou môže šíriť falošné VLAN identifikátory a spôsobiť nefunkčnosť siete, veľa možných VTP útokov kvôli zraniteľnostiam	Vypnutie MVRP. MRP, GARP, VTP po úspešnej propagácii VLAN	C	C	DIST COLDISTACC ACC	Lan Switch Security [2]
7	VTP musí byť používané	Uprednostniť VTP verzie 3, špecifikovať skryté heslo a zapnúť VTP pruning pokiaľ musí byť VTP zapnuté	C	C	DIST COLDISTACC ACC	Lan Switch Security [2]
8	Vysoké zaťaženie linky	Poslanie notifikácie pri prekročení prahovej hodnoty zaťaženia linky	C	M	A	Cisco SAFE Reference Guide [20]

Tab. 4.12: Odporúčania pre VLAN

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
1	Zlyhanie zariadenia alebo linky môže viesť k nefunkčnosti siete	Povolenie FHRP s autentizáciou a aktuálnou verziou	C	M	CORE/EDGE COLCOREDIST COLALL	CCNA Routing and Switching Study Guide [8]
2	Nepoužívané, staré a nezabezpečené služby môžu byť použité na škodlivé účely	Vypnutie nepoužívaných služieb z bezpečnostných dôvodov a na šetrenie CPU a pamäte	*1	H	*1	Cisco IOS features that you should disable or restrict [37]
3	Odpočúvanie komunikácie cez nezabezpečené tunely	Vypnúť tunely ktoré nie sú zabezpečené alebo zabezpečiť tunely	D	C	CORE/EDGE DIST COLCOREDIST COLDISTACC COLALL	CIS Cisco IOS 15 Benchmark [10] Cisco router configuration handbook [45]
4	Môže byť zneužitý odpočúvanie pokiaľ sa používa monitorovanie prevádzky a monitorovanie prevádzky kvôli legislatívnym potrebám	Monitorovanie výkonnosti siete a zber sieťového prenosu kvôli legislatívnym potrebám	C	N	A	Cisco Guide to Harden Cisco IOS Devices [7]
5	Útočník s fyzickým prístupom k zariadeniu alebo portu môže odpočúvať alebo posielat škodlivý obsah	Explicitne zakázať nepoužívané porty	D	C	A	Cisco Router Hardening [19] Network Security Auditing [5]
6	Zdrojové rozhranie pre management a control protokoly	Vytvoriť Loopback rozhranie s IP adresou	M/C	M	A	Cisco Guide to Harden Cisco IOS Devices [7] CIS Cisco IOS 15 Benchmark [10]
7	Pretečenie pamäte	Povoliť mechanizmy na detekciu pretečenia pamäte	M	M	A	Cisco Guide to Harden Cisco IOS Devices [7]

Riadok č.	Útok / Problém	Mitigácia / Nastavenie	Plane	Severity	Facility layer	Zdroj
8	Načítanie škodlivej konfigurácie zo siete počas bootovania	Vypnutie načítania operačného systému alebo konfigurácie zo siete pokiaľ to nie je nutné	M	M	A	Hardening Cisco Routers [44]
9	Odpočúvanie konfigurácií zariadení pri zálohe	Zapnutie zabezpečenej zálohy na server (SFTP, SCP)	M	H	A	Cisco Guide to Harden Cisco IOS Devices [7]
10	Vymazanie konfigurácie	Zapnutie ochrany pred výmazom konfigurácie	M	H	A	Cisco CCNA Security Study Guide [3]
11	Možnosť urobiť diff zmien konfigurácií a jej návrat	Periodické zálohovanie konfigurácie a logovanie jej zmien	M	M	A	Cisco CCNA Security Study Guide [3] Cisco Guide to Harden Cisco IOS Devices [7]
12	Nemožnosť prihlásenia pri zaseknutom TCP spojení	Terminovanie zaseknutého TCP spojenia	M	M	A	Cisco Guide to Harden Cisco IOS Devices [7]
13	Možnosť prečítať heslá z uniknutých konfigurácií	Zašifrovanie hesiel v otvorenej podobe	M	C	A	CIS Cisco IOS 15 Benchmark [10]

Tab. 4.13: Ostatné nezatriedené odporúčania

¹Záleží na výrobcovi, operačnom systéme a verzii

5 Implementácia

5.1 Použité technológie

5.1.1 Python

niečo o pythone, výhody, prečo je vhodný a bol vybraný

5.1.2 YAML

čo je, porovnať s XML, JSON, vlastnou syntaxou, prečo je YAML vhodný

5.1.3 Regulárne výrazy

nejaký obkec okolo (krátko), prečo sú vhodné, ako budú použité

5.2 Konfiguračné súbory

možno do implmentácie, automaticke zistovaine niektorých atributov

5.2.1 Súbor popisujúci zariadenie

device.yaml

5.2.2 Súbor popisujúci modul

module.yaml false positive, akceptovanie rizika

5.3 Moduly

Záver

Zhrnutie práce.

Literatúra

- [1] MILKOVICH, Devon. 13 Alarming Cyber Security Facts and Stats. In: *Cybint* [online]. 3.12.2018 [cit. 2019-11-08]. Dostupné z: <https://www.cybintsolutions.com/cyber-security-facts-stats/>
- [2] VYNCKE, Eric a Christopher PAGGEN. *LAN switch security: What hackers know about your switches*. Indianapolis, IN: Cisco Press, 2008. ISBN :978-1-58705-256-9.
- [3] MCMILLAN, Troy. *CCNA security study guide: exam 210-260*. Indianapolis, Indiana: Sybex, a Wiley Brand, 2018. ISBN 978-111-9409-939.
- [4] STALLINGS, William. *Network security essentials: applications and standards*. 4th ed. Boston: Prentice Hall, 2011. ISBN 978-0-13-610805-4.
- [5] JACKSON, Chris. *Network security auditing*. Indianapolis, IN: Cisco Press, 2010. Cisco Press networking technology series. ISBN 978-1-58705-352-8.
- [6] Guide for Conducting Risk Assessments: NIST Special Publication 800-30. In: *NIST* [online]. 2012 [cit. 2019-11-08]. Dostupné z: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
- [7] SINGH, Shashank. Cisco Guide to Harden Cisco IOS Devices. In: *Cisco* [online]. 2018 [cit. 2019-11-02]. Dostupné z: <https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>
- [8] LAMMLE, Todd. *CCNA: routing and switching : study guide*. Indianapolis, Indiana: SYBEX, [2013]. ISBN 978-1-118-74961-6.
- [9] PEPELNJAK, Ivan. Management, Control and Data Planes in Network Devices and Systems. In: *IpSpace* [online]. 2013 [cit. 2019-11-17]. Dostupné z: <https://blog.ipspace.net/2013/08/management-control-and-data-planes-in.html>
- [10] CIS Cisco IOS 15 Benchmark. In: *Center For Internet Security* [online]. 2015 [cit. 2019-11-02]. Dostupné z: <https://www.cisecurity.org/benchmark/cisco/>
- [11] BARKER, Elaine a Allen ROGINSKY. Transitioning the Use of Cryptographic Algorithms and Key Lengths. In: *NIST* [online]. 2019 [cit. 2019-11-02]. Dostupné z: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf>
- [12] Special-Purpose IP Address Registries. In: *IETF* [online]. [cit. 2019-12-08]. Dostupné z: <https://tools.ietf.org/html/rfc6890>
- [13] Updates to the Special-Purpose IP Address Registries. In: *IETF* [online]. [cit. 2019-12-08]. Dostupné z: <https://tools.ietf.org/html/rfc8190>
- [14] Special-Use IPv6 Addresses. In: *IETF* [online]. [cit. 2019-12-08]. Dostupné z: <https://tools.ietf.org/html/rfc5156>

- [15] GRÉGR, Matěj a Tomáš PODERMAŇSKI. Bezpečné IPv6: vícehlavý útočník. In: *ROOT.CZ* [online]. 26.2.2015 [cit. 2019-11-02]. Dostupné z: <https://www.root.cz/clanky/bezpecne-ipv6-vicehlavy-utocnik/>
- [16] PODERMAŇSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: trable s hlavičkami. In: *ROOT.CZ* [online]. 19.2.2015 [cit. 2019-11-02]. Dostupné z: <https://www.root.cz/clanky/bezpecne-ipv6-trable-s-hlavickami/>
- [17] KHANDELWAL, Manjul. OSPF Security: Attacks and Defenses. In: *SANOG* [online]. 2016 [cit. 2019-11-04]. Dostupné z: https://www.sanog.org/resources/sanog28/SANOG28-Tutorial_OSPF-Security-Attacks-and-Defences-Manjul.pdf
- [18] Understanding BGP TTL Security. In: *PacketLife* [online]. 2009 [cit. 2019-11-30]. Dostupné z: <https://packetlife.net/blog/2009/nov/23/understanding-bgp-ttl-security/>
- [19] GRAESSER, Dana. Cisco Router Hardening Step-by-Step. In: *SANS Institute* [online]. 2001 [cit. 2019-11-02]. Dostupné z: <https://www.sans.org/reading-room/whitepapers/firewalls/paper/794>
- [20] Cisco SAFE Reference Guide. In: *CIscO* [online]. San Jose, CA, 8. Júl 2018 [cit. 2019-11-02]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.pdf
- [21] NTP Amplification DDoS Attack. In: *Cloudflare* [online]. [cit. 2019-12-01]. Dostupné z: <https://www.cloudflare.com/learning/ddos/ntp-amplification-ddos-attack/>
- [22] The NTP FAQ and HOWTO. In: *Network Time Protocol* [online]. [cit. 2019-12-01]. Dostupné z: <http://www.ntp.org/ntpfaq/NTP-s-algo-crypt.htm>
- [23] VLAN Hopping: How to Prevent an Attack. In: *AT&T Cybersecurity* [online]. 2018 [cit. 2019-12-03]. Dostupné z: <https://www.alienvault.com/blogs/security-essentials/vlan-hopping-and-mitigation>
- [24] SATRAPA, Pavel. *IPv6: internetový protokol verze 6*. 4. aktualizované a rozšířené vydání. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-808-8168-430.
- [25] Bezpečné IPv6: příliš mnoho sousedů. In: *ROOT.CZ* [online]. 2015 [cit. 2019-12-08]. Dostupné z: <https://www.root.cz/clanky/bezpecne-ipv6-prilis-mnoho-sousedu/>
- [26] ALSADEH, Ahmad. Augmented SEND: Aligning Security, Privacy, and Usability. In: *RIPE NCC* [online]. 12.5.2015 [cit. 2019-11-02]. Dostupné z: <https://ripe70.ripe.net/presentations/67-RIPE70-SEND.pdf>
- [27] GRÉGR, Matěj a Tomáš PODERMAŇSKI. Bezpečné IPv6 : směrovač se hlásí. In: *ROOT.CZ* [online]. 5.2.2015 [cit. 2019-11-02]. Dostupné z: <https://www.root.cz/clanky/bezpecne-ipv6-smerovac-se-hlasi/>

- [28] PODERMAŇSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: zkrocení zlých směrovačů. In: *ROOT.CZ* [online]. 12.2.2015 [cit. 2019-11-02]. Dostupné z: <https://www.root.cz/clanky/bezpecne-ipv6-zkroceni-zlych-smerovacu/>
- [29] Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery. In: *IETF* [online]. [cit. 2019-12-08]. Dostupné z: <https://tools.ietf.org/html/rfc6980>
- [30] PODERMAŇSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: když dojde keš. In: *ROOT.CZ* [online]. 12.3.2015 [cit. 2019-11-02]. Dostupné z: <https://www.root.cz/clanky/bezpecne-ipv6-kdyz-dojde-kes/>
- [31] PODERMAŇSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: když dojde keš — obrana. In: *ROOT.CZ* [online]. 19.3.2015 [cit. 2019-11-02]. Dostupné z: <https://www.root.cz/clanky/bezpecne-ipv6-kdyz-dojde-kes-obrana/>
- [32] PODERMAŇSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: trable s multicastem. In: *ROOT.CZ* [online]. 5.3.2015 [cit. 2019-11-02]. Dostupné z: <https://www.root.cz/clanky/bezpecne-ipv6-trable-s-multicastem/>
- [33] REY, Enno, Antonios ATLASIS a Jayson SALAZAR. MLD Considered Harmful. In: *RIPE NCC* [online]. 2016 [cit. 2019-11-02]. Dostupné z: https://ripe72.ripe.net/presentations/74-ERNW_RIPE72_MLD_Considered_Harmful_v1_light_web.pdf
- [34] IPv6 First-Hop Security Configuration Guide. In: *Cisco* [online]. San Jose [cit. 2019-11-02]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-1sg/ip6f-15-1sg-book.pdf
- [35] BOUŠKA, Petr. Cisco IOS 11 - IEEE 802.1x, autentizace k portu, MS IAS. In: *SAMURAJ-cz* [online]. 2007 [cit. 2019-12-09]. Dostupné z: <https://www.samuraj-cz.com/clanek/cisco-ios-11-ieee-802-1x-autentizace-k-portu-ms-ias/>
- [36] BOUŠKA, Petr. *Cisco IOS 12 - IEEE 802.1x a pokročilejší funkce* In: *SAMURAJ-cz* [online]. 2007 [cit. 2019-11-02]. Dostupné z: <https://www.samuraj-cz.com/clanek/cisco-ios-12-ieee-802-1x-a-pokrocilejsi-funkce/>
- [37] MOLENAAR, René. Cisco IOS features that you should disable or restrict. In: *NetworkLessons.com* [online]. [cit. 2019-11-02]. Dostupné z: <https://networklessons.com/uncategorized/cisco-ios-features-that-you-should-disable-or-restrict>
- [38] BOUŠKA, Petr. Cisco IOS 23 - Autentizace uživatele na switchi vůči Active Directory. In: *SAMURAJ-cz* [online]. 2009 [cit. 2019-11-02]. Dostupné z: <https://www.samuraj-cz.com/clanek/cisco-ios-23-autentizace-uzivatele-na-switchi-vuci-active-directory/>
- [39] VYNCKE, Erik. ND on wireless links and/or with sleeping nodes. In: *IETF* [online]. [cit. 2019-11-02]. Dostupné z: <https://www.ietf.org/proceedings/89/slides/slides-89-v6ops-3.pdf>

- [40] VYNCKE, Erik. IPv6 First Hop Security: the IPv6 version of DHCP snooping and dynamic ARP inspection. In: *Slidde Share* [online]. 2012 [cit. 2019-11-02]. Dostupné z: <https://www.slideshare.net/IKTNorge/eric-vyncke-layer2-security-ipv6-norway>
- [41] GREGR, Matej, Petr MATOUSEK, Miroslav SVEDA a Tomas PODERMANSKI. Practical IPv6 monitoring-challenges and techniques. In: *12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011) and Workshops*. IEEE, 2011, 2011, s. 650-653. DOI: 10.1109/INM.2011.5990647. ISBN 978-1-4244-9219-0. Dostupné také z: <http://ieeexplore.ieee.org/document/5990647/>
- [42] MARTIN, Tim. IPv6 Sys Admin Style. In: *SlideShare* [online]. 2016 [cit. 2019-11-02]. Dostupné z: <https://www.slideshare.net/tjmartin2020/ipv6-sysadmins-63071235>
- [43] SAFE Overview Guide: Threats, Capabilities, and the Security Reference Architecture. In: *Cisco* [online]. Január 2018 [cit. 2019-11-02]. Dostupné z: <https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-overview-guide.pdf>
- [44] AKIN, Thomas. *Hardening Cisco routers*. Sebastopol: O'Reilly, 2002. ISBN 05-960-0166-5.
- [45] HUCABY, Dave, Steve MCQUERRY, Andrew WHITAKER a Dave HUCABY. *Cisco router configuration handbook*. 2nd ed. Indianapolis, IN: Cisco Press, 2010. ISBN 978-1-58714-116-4.
- [46] Port Knocking. In: *Mikrotik* [online]. [cit. 2019-12-09]. Dostupné z: https://wiki.mikrotik.com/wiki/Port_Knocking
- [47] DOOLEY, Kevin a Ian J. BROWN. *Cisco IOS cookbook*. 2nd ed. (Revised and updated). Sebastopol, CA: O'Reilly, 2007. ISBN 05-965-2722-5.
- [48] Protocol-Independent Routing Properties Feature Guide. In: *Juniper* [online]. 2019 [cit. 2019-12-09]. Dostupné z: https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/router-id-edit-routing-options.html
- [49] TISO, John a Keith HUTTON. *Designing Cisco network service architectures (ARCH)*. 3rd ed. Indianapolis, IN: Cisco Press, 2012. ISBN 15-871-4288-0.
- [50] Cisco Config Analysis Tool. *GitHub* [online]. [cit. 2019-12-11]. Dostupné z: <https://github.com/cisco-config-analysis-tool/ccat>
- [51] Router connectivity visualization and compliance auditing. *GitHub* [online]. [cit. 2019-12-11]. Dostupné z: <https://github.com/asifhj/Router-Auditing-Tool>

Zoznam symbolov, veličín a skratiek

CIA	confidentiality, integrity, availability – dôvernosc, integrita, dostupnost
DDoS	Distributed Denial of Service – distribuované odoprenie služby
DoS	Denial of Service – odoprenie služby
ACL	Access Control List – zoznam pre riadenie prístupu
CVSS	Common Vulnerability Scoring System
IDS	Intrusion Detection System – systém detekcie narušenia
IPS	Intrusion Prevention System – systém prevencie prienikov
FHRP	First Hop Redundancy Protocol
SNMP	Simple Network Management Protocol
AAA	Authentication Authorization Accounting
SSH	Secure Shel
OSPF	Open Shortest Path First
LAN	Local Area Network
IP	Internet Protocol
IPv6	Internet Protocol version 6
VLAN	Virtual LAN
ARP	Address Resolution Protocol
MAC	Media Access Control
LLDP	Link Layer Discovery Protocol
CDP	Cisco Discovery Protocol
API	Application programming interface
GUI	graphical user interface – grafické užívateľské rozhranie
uRPF	Unicast Reverse Path Forwarding
BGP	Border Gateway Protocol
TTL	Time To Live
HTTP	Hypertext Transfer Protocol
NTP	Network Time Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
PTP	Precision Time Protocol
SCP	Secure Copy Protocol
TFTP	Trivial File Transfer Protocol
SFTP	Secure File Transfer Protocol
ICMP	Internet Control Message Protocol
VPN	Virtual Private Network – Virtuálna privátne sieť
PPTP	Point-to-Point Tunneling Protocol

L2TP	Layer 2 Tunneling Protocol
IPSec	IP Security
MLD	Multicast Listener Discovery
IGMP	Internet Group Management Protocol
VRRP	Virtual Router Redundancy Protocol
HSRP	Hot Standby Redundancy Protocol
GLBP	Gateway Load Balancing Protocol
STP	Spanning Tree Protocol
DTP	Dynamic Trunking Protocol
EAP	Extensible Authentication Protocol
PEAP	Protected Extensible Authentication Protocol
EAPoL	Extensible Authentication Protocol over LAN
VTP	Virtual Trunking Protocol
MVRP	Multiple VLAN Registration Protocol
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
SEND	Secure Neighbor Discovery

Zoznam príloh

A	Zdrojové súbory	80
A.1	Konfiguračné súbory	80
B	Checklist	81

A Zdrojové súbory

A.1 Konfiguračné súbory

B Checklist